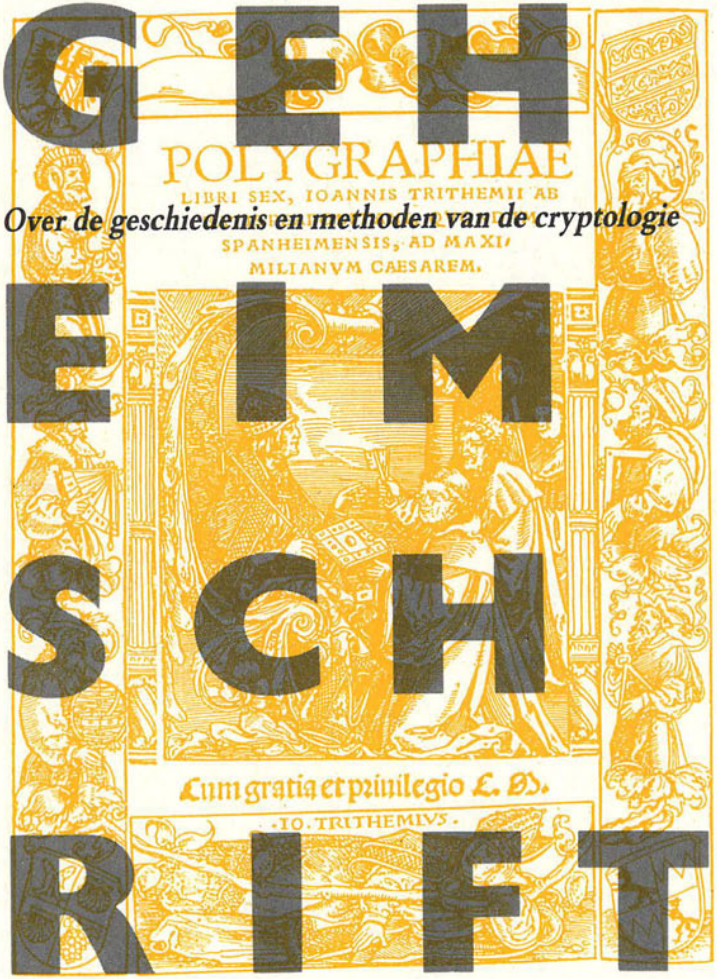
*'A man is crazy, who writes a secret in any other way than one which will conceal it from the vulgar'*
*(Roger Bacon)*

# GEHEIMSCHRIFT

*Over de geschiedenis en methoden van de cryptologie*




Scryption

# INLEIDING

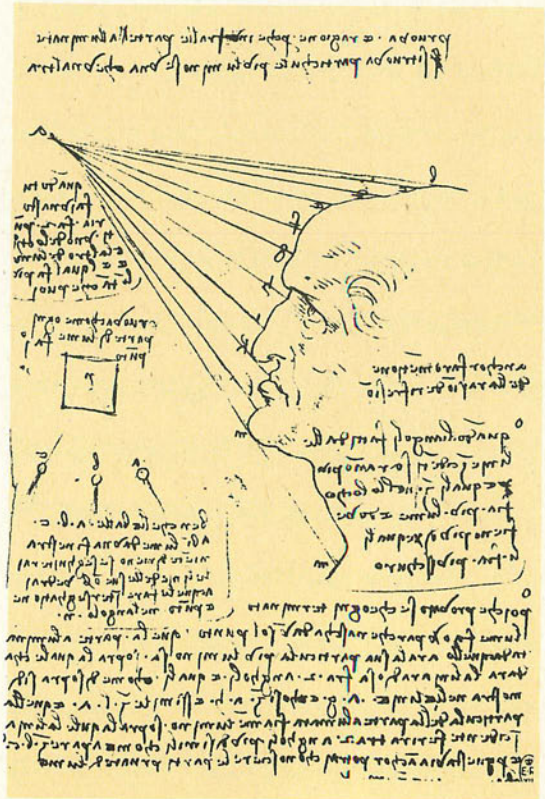
***De vroegste vormen van schrift waren voor de meeste mensen eigenlijk als een soort 'geheimschrift'. Slechts weinigen konden in die begintijd immers de tekens lezen. Naarmate het schrift zich verder ontwikkelde en door steeds meer mensen begrepen werd zocht de mens naar nieuwe manieren om geheime boodschappen zo op te schrijven dat een buitenstaander ze niet kon lezen; een proces dat zich in vrijwel alle culturen heeft voorgedaan.***
***Ook geheimschrift blijkt van alle tijden te zijn.***

***In de eerste vierduizend jaar van het bestaan van het schrift (± van 2600 v.Chr. tot ± 1400 n.Chr.) is er geen sprake van een doorlopende ontwikkeling van het geheimschrift. De gevallen van het gebruik van geheimschrift staan los van elkaar en ontstaan, bloeien en verdwijnen met de opkomst en ondergang van de verschillende beschavingen. Pas in de vroege renaissance (15e eeuw) wordt er een basis gelegd voor een ontwikkeling in cryptografische systemen, die zich heeft doorgezet tot in onze eeuw.***

***Kenmerken van perfecte geheimschriften: '...dat ze niet bewerkelijk zijn om te schrijven en te lezen; dat ze onmogelijk te ontcijferen zijn; en dat ze, in sommige gevallen, boven elke verdenking staan.' (Francis Bacon)***

## *Verklaring van enkele veel gebruikte termen in dit boek*

| | |
|---|---|
| **cryptografie** | het omzetten van een leesbare tekst in geheimschrift |
| **cryptanalyse** | het ontcijferen van een in geheimschrift geschreven tekst het kraken van een geheimschrift |
| **cryptologie** | de wetenschap, die zich bezighoudt met de cryptografie (het coderen) en de cryptanalyse (het decoderen) |
| **cryptogram** | een in geheimschrift geschreven tekst |
| **klare tekst** | een gewone leesbare tekst (dus niet in geheimschrift) |
| **cijfer** | een symbool (letter of getal) ter vervanging van een klare-tekst-letter |
| **sleutel** | het systeem waarmee de klare tekst in geheimschrift is gezet |
| **code** | geheimschrift, ook wel letters of getal ter vervanging van een woord |
| **sleutelwoord** | een woord, dat bekend is aan zowel de zender als de ontvanger en dat aangeeft hoe het geheimschrift opgelost moet worden |
| **frequentieanalyse** | onderzoek naar hoe vaak iedere letter van een alfabet in een bepaalde taal voorkomt. Zie ook op pagina 6. |
| **monoalfabetische vervanging** | een vervangingssysteem waarbij elke letter van het alfabet door een vaste andere letter wordt vervangen |
| **polyalfabetische vervanging** | een systeem waarbij voor elk deel van een bericht, of zelfs voor elke letter een ander cijferalfabet gebruikt wordt om de geheimschriftletters uit te halen. |



*Een van de meest bekende geheimschriften is dat van Leonardo da Vinci: hij schreef alles in spiegelschrift. Hier (in geel) een fragment van een studieblad over de lichtval op het menselijk gezicht.*

# Het Begin: Mesopotamië

Op zichzelf is het spijkerschrift dat door de Sumeriërs in Mesopotamië werd gebruikt al als een geheimschrift te beschouwen, omdat het slechts door een kleine groep ingewijden werd gebruikt.
Toch was er rond 2600 v.Chr. in Zuid-Mesopotamië een echt geheimschrift in gebruik: sommige tekens werden vervangen door tekens die wel bekend waren, maar die in die strekking nooit voorkwamen.

Dit geheimschrift heette UD GAL NUN, wat de vervanging was voor AN EN LÍL (de god ENLIL). Dit UD GAL NUN-schrift werd gebruikt in rituele klaagzangen en was alleen bestemd voor ingewijden. Het is de oudste vorm van geheimschrift die wij kennen.

bv. An = god,



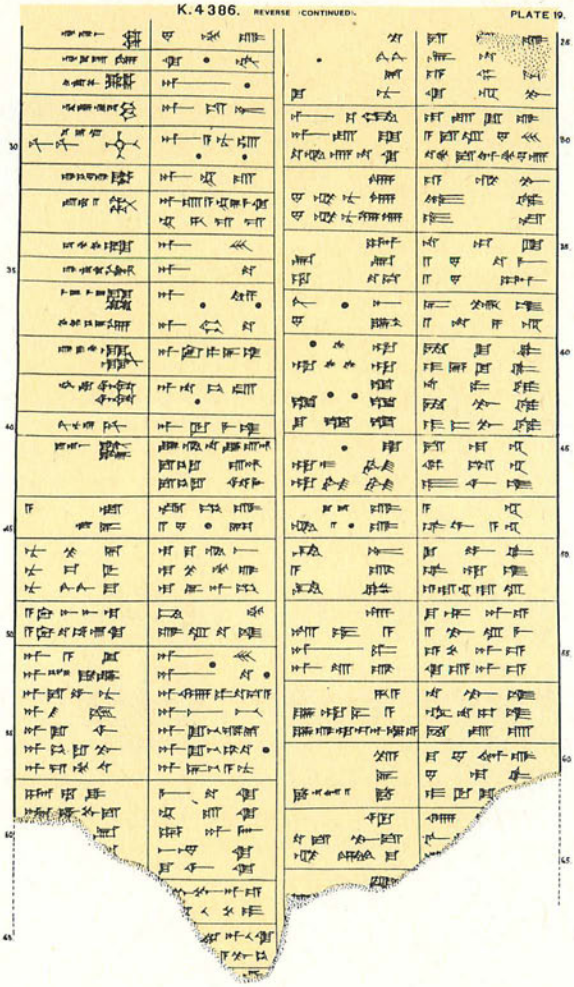
werd vervangen door

Ud = zon, dag

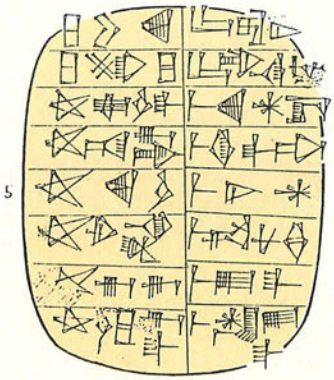


Bij de erediensten werd vanaf ± 1900 v.Chr. een geheime taal gebruikt, die Emesal, vrouwentaal, werd genoemd, naar de – oorspronkelijk homoseksuele – cultische zangers, de 'galla'. Het Emesal bleef zo'n tweeduizend jaar in gebruik en werd later het 'kerklatijn' van de Sumeriërs.

Aan het eind van het spijkerschrift-tijdperk, tussen 770 v.Chr. en het begin van de jaartelling, verving men woorden en godennamen wel eens door getallen: bijv. 30 = maangod (30 dagen); 20 = weergod. Men hoopte zo achter de betekenis van de woorden, de namen en de goden zelf te komen. Dit is eigenlijk meer een geheim van de taal dan een geheimschrift en te vergelijken met de kabbala, die zich bezighoudt met de getalswaarde en de diepere betekenis van de woorden in het Oude Testament.
Schrijvers vervingen ook wel hun eigen namen door cijfers, misschien uit vermaak of om op te vallen.




*Een schrift van tekenclusters uit de bibliotheek van Assjurbanipal met godennamen en daarnaast de echte uitspraak (7e eeuw v. Chr.). Het doel ervan is niet duidelijk; de tekens zijn te lezen, maar de combinaties, die pictogrammen vormen, zijn onbekend. Het lijkt op het 'lezen' van olievlekken in water of van vlekjes op de lever van geslachte dieren, die de Mesopotamiërs als schrifttekens beschouwden. Met dit soort methoden wilden de Mesopotamiërs het onbegrijpelijke begrijpen.*



*Tablet uit Jena met 2 schriftsoorten: links geheim- en rechts gewoon schrift.*

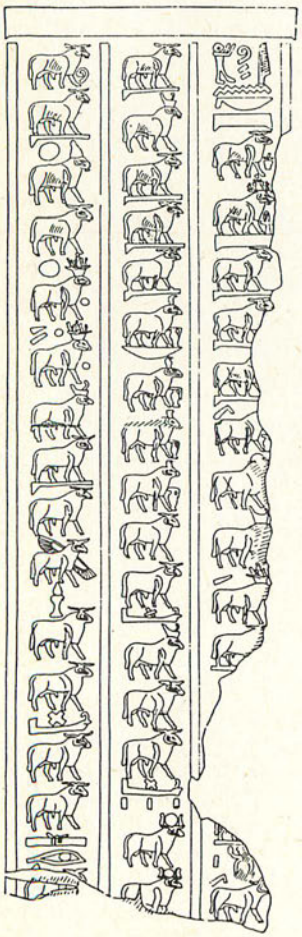
# Egypte: Van Krokodillen en Scarabeeën



Ook het hiëroglyphenschrift van de Egyptenaren werd slechts door een kleine groep – de priesters – gelezen. Het geheime karakter wordt nog versterkt doordat het voor een deel een schrift in rebusvorm is: 'licht' wordt bijvoorbeeld voorgesteld door een tekening van een knots, omdat de beide woorden dezelfde medeklinkers hebben en het Egyptische schrift, net als de semitische talen, slechts medeklinkers kent.
Bovendien staan de tekens in het hiëroglyphenschrift niet altijd in een voor ons logische volgorde: voor de Egyptenaren, die erg van hun schrift hielden, was het belangrijker, dat de tekens fraai bij elkaar stonden. Ook de schrijfrichting veranderde als dat zo mooier uitkwam. Zo moest de lezer altijd een beetje puzzelen op een tekst.

*Dit beeld van Ramses II kan als een grote, ruimtelijke hiëroglyph van de naam van de farao worden gelezen.*

*Ram-hiëroglyphen uit de tempel van Esna.*



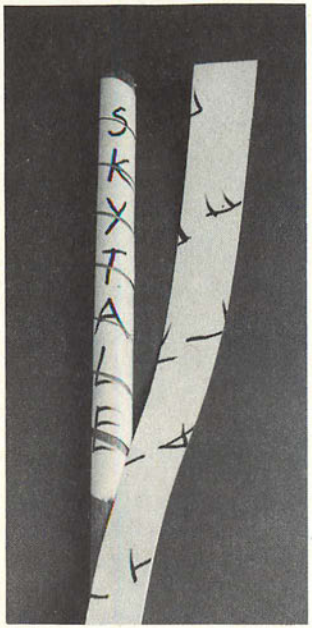
*Boven- (links) en onderkanten van scarabeeën met cryptische faraonamen.*

In de Egyptische stad Menet Choefoe verving rond 1900 v.Chr. een meesterschrijver in een tekst over het leven van zijn meester een aantal hiëroglyphen door andere, minder gebruikte tekens. Zo vestigde hij meer aandacht op de tekst en maakte hiermee een van de oudst bekende voorbeelden van geheimschrift.
Deze wijze van vervanging werd steeds vaker toegepast in de zogenaamde 'begrafenis-cryptografie'. Op beelden en deurposten in tempels en graven bracht men 'geheime' nieuwe tekens aan, bestaande uit nieuwe samenstellingen van oude tekens. De schrijvers deden dit niet zozeer om een betekenis te verbergen, als wel om de lezer nieuwsgierig te maken, zodat hij moeite zou doen om de naam van de dode te spellen en hem hardop uit te spreken. Daardoor zouden de beschreven zegeningen naar de ziel van de overledene gaan. Op den duur werden deze geschriften echter zo gecompliceerd, dat deze hun doel misten: de lezer liep er aan voorbij.

Uit de 2e eeuw na Chr. stammen teksten uit de tempel van Esna, die onder andere gewijd was aan de krokodillengod Scemanefer en aan de ram-god Chnoem. Deze teksten bestaan vrijwel helemaal uit hiëroglyphen in de vorm van krokodillen of rammen die, in combinatie met andere tekens, veranderen van klank of betekenisen die alleen begrepen konden worden door de priesters van deze tempel.

Op de onderkant van de scarabeeën, stenen in de vorm van kevers, die door de Egyptenaren veelvuldig als sieraad werden gedragen, stonden vaak de hiëroglyphen van de naam van een farao. Deze tekens werden geheime tekens omdat alleen aan ingewijden bekend was dat ze ook als de naam van een god konden worden gelezen.
Zo is bijvoorbeeld Mencheperré de troonnaam van de beroemde farao Thoetmosis III. Maar de hiëroglyphen voor deze naam zijn ook te lezen als Amon, de belangrijkste god in het Nieuwe Rijk. Amon is de verborgene, de god die overal in is, vandaar dat zijn naam in andere namen werd verborgen.

# Alle Geheimen op een Stokje



*De skytale.*

Het waren de Spartanen die in de 5e eeuw v.Chr. het eerste militaire cryptografische systeem ontwikkelden. Zij gebruikten de 'skytale', het eerste hulpstuk of 'apparaat' in de geschiedenis van de cryptologie. De 'skytale' is een stok waaromheen een lange strook papyrus, leer of perkament werd gewikkeld, zodat de hele stok bedekt werd. De geheime boodschap werd over de gehele lengte van de stok op deze strook geschreven, waarna de strook werd afgewikkeld en opgestuurd. De ontbonden letters werden pas weer leesbaar nadat de strook weer om een stok van dezelfde dikte werd gewikkeld.

Aeneas de Thraciër wijdde in zijn militair wetenschappelijke boek 'Over de verdediging van versterkte plaatsen' een heel hoofdstuk aan veilige communicatie. Hij gaf een lijst van diverse systemen, zoals de vervanging van klinkers door stippen (alpha = 1 stip, epsilon = 2 stippen, tot omega = 7 stippen), terwijl de medeklinkers niet vervangen worden.

Een ander systeem van Aeneas werd nog in deze eeuw door Duitse spionnen in de Tweede Wereldoorlog gebruikt: het prikken van gaatjes in een boek onder of boven de letters die samen de geheime boodschap vormen.

Polybius, een andere Griekse schrijver, zette voor het eerst letters om in cijfers met behulp van een vierkante tabel. Elke letter wordt door twee cijfers vervangen, bijv. A = 11, C = 13, T = 44, R = 42, X = 53 enz.
Polybius' vierkant wordt het 'schaakbord' genoemd en ligt aan de basis van vele latere cijfersystemen.

Polybius sprak ook over de mogelijkheid de cijfers door te seinen over een grote afstand met behulp van toortsen. Bijvoorbeeld: 1 toorts rechts en 4 toortsen links = d.

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

*Het 'schaakbord' van Polybius*

## India

**De Kama Sutra noemt geheimschrift als een van de 64 yoga's die een vrouw moet kunnen beoefenen. Cryptografie staat er als 45ste op de lijst, die begint met zang en die ook het oplossen van woordpuzzels en raadselpoëzie bevat.**

## Het Caesar-Alfabet

Het eerste bewijs dat geheimschrift ook werkelijk werd gebruikt voor militaire doeleinden vinden we in het boek van Julius Caesar over de Gallische oorlogen. Hij beschrijft hoe zijn brief, bevestigd aan een speer, het Romeinse kamp binnengegooid werd. De brief werd daarop door Cicero ontcijferd. Het geheimschrift waar de Romeinse veldheer zich van bediende ging de geschiedenis in als het 'Caesar-alfabet', en bestond uit het drie plaatsen opschuiven van alle letters van het alfabet.

OMNIA GALLIA EST DIVISA IN PARTES TRES wordt dan, uitgaande van een 26-letterig alfabet: RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV.
Caesar schijnt de letters ook wel in een gecompliceerder systeem te hebben omgezet, terwijl Augustus, de eerste keizer van Rome, genoegen nam met het slechts één plaats opschuiven van de letters van het alfabet.

## Atbasch

Ook in de Bijbel komen we lettervervanging tegen. Zo lezen we in Jeremia 25:26 en 51:41 de naam Sheshach waar Babylon (Babel) wordt bedoeld, terwijl twee regels verderop wel de naam Babylon gebruikt wordt.

ren ter slachtbank, als rammen en
als bokken.
41 Hoe is ♭Sesach veroverd, en de roem b J
der geheele wereld ingenomen! Hoe 26.
is Babel tot eene verwoesting geworden
42 onder de volken! Eene zee i. over Babel e l
gegaan, en door de veelheid harer
43 golven is zij bedekt; hare steden zijn
tot eene woestijn en tot een dor, een-
zaam land geworden; tot een land,
waarin niemand woont en waar geen
44 mensch doortrekt. Want ik heb Bel

De naam Sheshach ontstaat door toepassing van het traditionele Hebreeuwse vervangingssysteem 'atbasch' op de naam Babel, waarbij de eerste letter van het geheel uit medeklinkers bestaande Hebreeuwse alfabet vervangen wordt door de laatste en omgekeerd, de tweede letter door de op-een-na-laatste, enzovoort.
'Atbasch' inspireerde de middeleeuwse monniken en schrijvers tot het gebruik van lettervervangingssystemen.

# Cryptanalyse in de Arabische Wereld

## Frequentieanalyse

6 **Om een cryptogram te kunnen kraken is onderzoek nodig naar hoe vaak iedere letter van een alfabet in de gebruikte taal voorkomt; hoe vaak in combinatie met andere letters, hoe vaak bepaalde uitgangen van woorden voorkomen, enz. Deze kenmerken worden bij cryptanalyse ook onderzocht in het te kraken geheimschrift, waarna de gevonden kenmerken met elkaar vergeleken worden, zodat de cryptanalist kan beginnen te gissen naar de betekenis van de meest voorkomende tekens in het geheimschrift.**

*Frequentieanalyse van de in het Nederlands voorkomende tekens.*

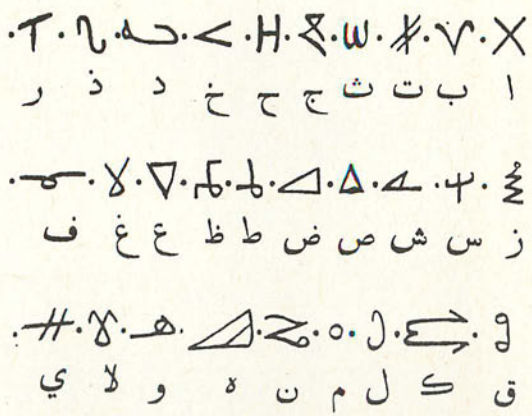
| | | | | | |
|---|---|---|---|---|---|
| *e* | *1586* | *h* | *232* | *.* | *76* |
| | *1425* | *v* | *223* | *f* | *70* |
| *n* | *858* | *m* | *188* | *j* | *25* |
| *a* | *633* | *k* | *187* | *-* | *10* |
| *t* | *556* | *u* | *159* | *y* | *8* |
| *r* | *542* | *w* | *130* | *;* | *4* |
| *d* | *512* | *p* | *123* | *:* | *4* |
| *o* | *482* | *c* | *123* | *x* | *3* |
| *i* | *467* | *b* | *119* | *'* | *2* |
| *s* | *351* | *z* | *116* | *?* | *2* |
| *l* | *310* | *y* | *107* | *q* | *1* |
| *g* | *282* | *,* | *82* | | |

Terwijl het overgrote deel van Europa zich in een chaotische en onrustige periode bevond kwam de Arabische cultuur in de Middeleeuwen tot grote bloei. Aangezien volgens de Koran afbeeldende kunsten verboden waren, hield men zich volop bezig met taal en schrift: woordraadsels, rebussen, anagrammen e.d. Grammatica werd een belangrijke studie, waarin ook geheimschrift behandeld werd.
Bovendien hielden de Arabische wetenschappers zich als eersten in de geschiedenis bezig met cryptanalyse: zij ontdekten en beschreven reeds goede methoden voor het schrijven in geheimschrift en het ontcijferen ervan.
Rond 1400 schreef Qalqashandi in Egypte een veertiendelige encyclopedie voor de secretarisklasse. Hij wijdt daarin een hoofdstuk aan vormen van correspondentie, waarin ook onzichtbare inkten, geheimschriften en cryptanalyse worden besproken.

Qalqashandi behandelt zeven cijfersystemen:
1. een letter wordt door een andere letter vervangen
2. een woord wordt van achteren naar voren geschreven
3. de letters in een woord worden om en om verwisseld
4. de letters worden als nummers geschreven, volgens het systeem, waarin Arabische letters een numerieke waarde hebben.
5. elke letter van een klare tekst wordt vervangen door twee Arabische letters, waarvan de gezamenlijke numerieke waarde gelijk is aan die van de klare tekst letter
6. elke letter wordt vervangen door de naam van een man
7. de letters worden vervangen door de maanstanden, landennamen, boomsoorten, getekende vogels of speciale symbolen.

In een soorgelijke lijst in een 10e-eeuws handboek voor de klasse van de secretarissen staat vermeld dat de vervanging door vogels en maanstanden uit Perzië afkomstig was.

Qalqashandi beschrijft stap voor stap de methode van cryptanalyse en de daarbij noodzakelijke frequentieanalyse:
- de cryptanalist moet eerst weten in welke taal het bericht is geschreven;
- de kenmerken van die taal moeten bekend zijn, zoals welke lettercombinaties nooit of zelden voorkomen en hoe vaak de letters van het gebruikte alfabet voorkomen.
- de letters van het bericht in code moeten worden geteld en de frequentie van ieder gebruikt symbool moet worden genoteerd;
- als de cryptograaf zo slim is geweest de verdeling in woorden te verbergen, moet het symbool dat tussen twee woorden staat gevonden worden. Begin met de eerste letter en ga ervan uit dat de volgende letter het woordverdelingssymbool is. Kijk dan hoe vaak dat symbool terugkomt en of dat een mogelijke verdeling in woorden oplevert. Is dat niet het geval, neem dan de volgende letter en ga zo door totdat een aannemelijke verdeling in woorden gevonden is.
- vergelijk nu de frequentie van de symbolen met die van de letters van het alfabet en vergelijk opeenvolgende symbolen met vaak opeenvolgende letters in het geheimschrift;
- vertaal als eerste woorden die uit twee letters bestaan. Probeer alle tweeletter-woorden uit totdat al deze woorden kloppen.
- schrijf nu de gevonden letters onder de corresponderende symbolen in de tekst.
- doe het voorgaande vervolgens met de drieletter-woorden, de vier- en de vijfletter-woorden
- probeer bij twijfel steeds andere combinaties uit totdat de hele tekst klopt.



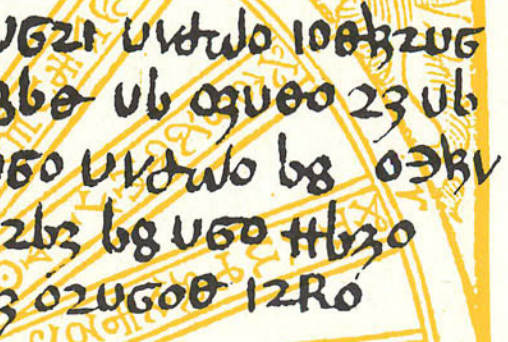
*Arabisch alfabet met vertaling in geheimschrift.*

Met het verval van de Arabische cultuur raakte ook deze kennis in de vergetelheid en moest het principe van de cryptanalyse weer door anderen en elders opnieuw worden uitgevonden.
Om informatie over belastingen geheim te houden was er vanaf de 16e eeuw bij de belastingambtenaren in Istanbul, Syrië en Egypte een geheimschrift in gebruik, het 'Qirmeh', wat bestond uit tekens, die afgeleid waren van vereenvoudigde en vervormde Arabische letters en afkortingen.

# In de Middeleeuwen

Na het ineenstorten van het Romeinse rijk vervallen de kunsten en wetenschappen en ook de toepassing van geheimschrift staat op een laag pitje. Hooguit zet af en toe een monnik ergens zijn naam of een notitie om in cijfers, om zichzef te vermaken, of uit verveling misschien.
De gebruikte systemen waren heel simpel: stippen in plaats van klinkers, griekse, hebreeuwse of armeense letters in plaats van de Romeinse, alle letters één plaats opschuiven, of op z'n hoogst letters vervangen door nieuwe tekens. Zo zou Bonifacius in de 8e eeuw cryptografische puzzels, gebaseerd op het vervangen van klinkers door stippen, in Noord-Europa hebben ingevoerd.
Paus Sylvester II maakte rond het jaar 1000 zijn notities in een kortschrift systeem, dat de Tyroonse noten wordt genoemd, naar de uitvinder ervan Tullius Tyro, een bevrijde slaaf van Cicero.

*Het prachtige eigenhandig geschreven geheimschrift van de Engelse amateur-astronoom Geoffrey Chaucer, uit zijn boek 'The Equatorie Of The Planetis' behoort tot de mooiste uit de geschiedenis.*



# Geheimschrift en Magie

Cryptologie is in de loop der eeuwen vaak geassocieerd met zwarte kunst, magische recepten en occultisme en werd daarom veelal met argwaan bekeken.
Aan het eind van het Romeinse rijk bedienden magiërs zich al van geheimschrift om hun kunsten voor de ogen van leken te verbergen.
En Plutarchus schrijft dat zeer oude orakels door de priesters in Delphi in geheimschrift werden bewaard.

Door dit soort praktijken werd en wordt cryptologie vaak in een adem genoemd met occulte manieren om het onbekende te verklaren: het lezen van vogelvluchten, van ingewanden van dieren, van handlijnen en koffiedikkijken.

Een van de beroemdste magische manuscripten is het 'Leidse papyrus', uit de 3e eeuw n.Chr., dat in Thebe werd gevonden en geschreven is in een late vorm van het Demotisch-grieks, een schriftvorm die uit uit het Egyptisch is ontstaan. Op dit papyrus staan de cruciale gedeelten van belangrijke recepten in geheimschrift geschreven, bijv.: 'wil je een huidziekte bij een man veroorzaken, zo, dat het niet zal genezen, neem dan een ...-hagedis en een ...-hagedis, kook ze met olie en was de man er mee', waarbij het woord huidziekte en de namen van de hagedissen in crypto geschreven staan.

Ook in de Middeleeuwen werd cryptografie vaak gebruikt voor magische doeleinden. En in de Renaissance zetten alchemisten de cruciale delen van formules vaak om in geheimschrift. Zo schrijft aan het einde van de 15e eeuw Arnaldus de Bruxella, een in Napels werkende alchemist, vijf regels in geheimschrift om de formule van het maken van de Steen Der Wijzen niet prijs te geven.

Rond 1590 beschuldigde de koning van Spanje, Philips II, de Fransen nog van het gebruik van zwarte magie, omdat ze zijn onkraakbaar geachte geheimschrift hadden gebroken. Philips, die hoopte dat de Fransen door de Paus bestraft zouden worden voor heidense praktijken, maakte zich aan het hof in Rome alleen maar belachelijk omdat hij niet op de hoogte was van het inmiddels in diplomatieke kringen algemene gebruik van cryptanalyse. De Paus bijvoorbeeld, had zelf meerdere geheimschriftkrakers in dienst.

*De schijnbare link tussen cryptologie en magie werd nog eens versterkt door het gebruik van voor leken mysterieuze tekens in de astrologie en de alchemie, zoals bij deze cijferschijf.*

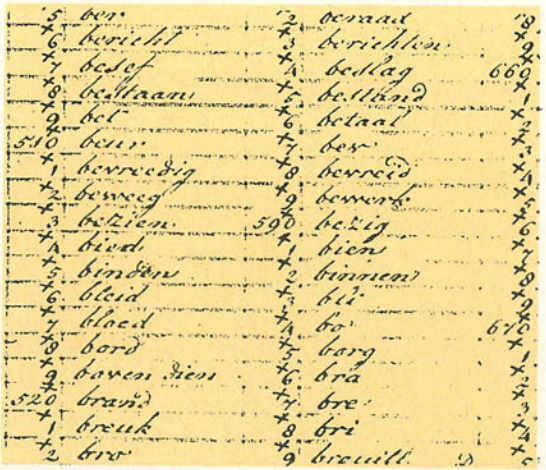
# Codeboeken

De cryptologie van na de Middeleeuwen maakt gebruik van twee basisvormen: 'cijfers' of vervanging van letters of woorden door codes. Dit laatste vond in diplomatieke kringen veel toepassing.

## Nomenclatuur

**De nomenclatuur combineert een cijferalfabet (de vervanging van letters door andere letters of cijfers) met een codelijst waarin woorden, lettergrepen of namen vervangen worden door getallen of lettercombinaties. Deze codelijsten groeiden uit van een dozijn woorden in de 14e eeuw tot een kleine drieduizend woorden en lettergrepen in de nomenclatuur van de Russische tsaar.**

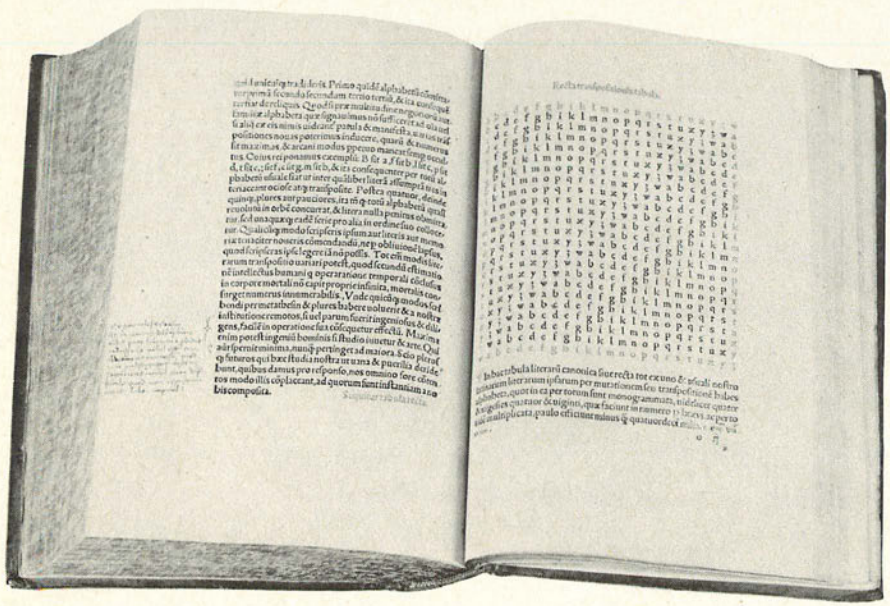




De vervanging van woorden door codes stamt deels af van het gebruik van afkortingen en deels van het gebruik van obcsure benamingen en beelden in orakels en magie.
Het oudste cryptografische document dat in de archieven van het Vaticaan is te vinden, een lijst van codes uit 1327 voor correspondentie in de strijd tussen de Gwelfen en Ghibelijnen, bevat beide soorten vervangingen:

O = 'officiale' (een hoge ambtenaar)
De Kinderen van Israël = Gwelfen en
Egyptenaren = Ghibelijnen

In 1379 liet de antipaus Clemens VII, die het jaar daarvoor naar Avignon was gevlucht, door zijn secretaris Gabrielle di Lavinde een nieuw geheimschrift maken. Dit bestond uit een serie van individuele sleutels voor zijn 24 correspondenten. Iedere sleutel bevatte naast een mono-alfabetisch vervangingsalfabet een lijst van veel gebruikte woorden met een tweeletter-code ter vervanging. Dit zijn de vroegste voorbeelden van het cryptografische systeem, dat de volgende 450 jaar in heel Europa en Amerika het meest gebruikt zou worden: de nomenclatuur.



*De Polygraphia van Trithemius uit 1506.*

# De Oude Boeken

Ook voor de cryptologie is de tijd van de Renaissance, de 15e en 16e eeuw, van grote betekenis. In deze periode herleeft de belangstelling voor de kennis die men in de oudheid al had op het gebied van kunsten en wetenschappen en die tijdens de roerige middeleeuwen verloren was gegaan of op de achtergrond geraakt.
Een aantal sleutelfiguren bestudeerde vele terreinen van de kunsten en wetenschappen en schreef boeken over zeer uiteenlopende onderwerpen, waaronder de cryptologie. Vooral Alberti, Trithemius, Porta, Cardano en Vigenère hebben toen de basis gelegd voor de moderne cryptologie. Voor het eerst in de geschiedenis van het geheimschrift ontstaat er een doorgaande ontwikkeling, die begint met de uitvindingen van deze schrijvers uit de Renaissance en die doorloopt tot in onze tijd.
Door de uitvinding van de boekdrukkunst in het midden van de 15e eeuw konden hun boeken bovendien in oplagen gedrukt en herdrukt worden, hetgeen bijgedragen heeft aan de verspreiding van de cryptologie in Europa.

# De Cijferschijf van Alberti

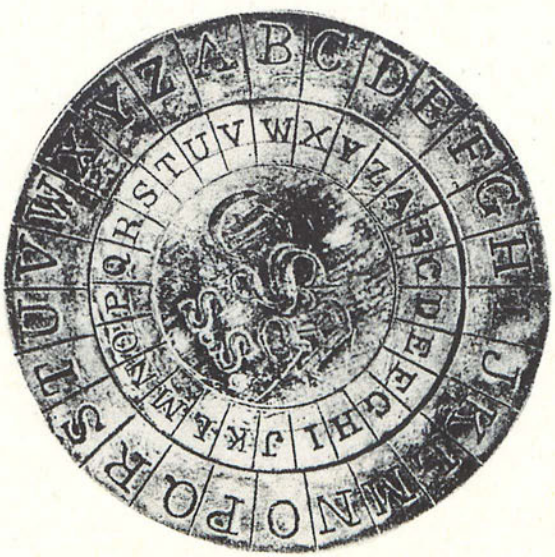
De eerste die een polyalfabetische sleutel bedacht was Leon Batista Alberti, een groot architect, atleet, kunstenaar en denker uit de 15e eeuw. In een artikel over cryptologie, waarin hij eerst ingaat op de cryptanalyse schrijft hij dat, om een goed – dus onkraakbaar – geheimschrift te maken men zich eerst moet verplaatsen in degene die het geheimschrift zal proberen te ontcijferen. Daarna beschrijft hij een sleutel die volgens hem onkraakbaar is. Deze zogenaamde cijferschijf was inderdaad lange tijd niet te kraken, hoewel na hem niemand de schijf meer gebruikte zoals hij het bedoeld had.

Op de buitenste ring van de schijf staan de letters van de klare tekst aangegeven in hoofdletters; op de binnenste ring, die kan draaien, staan de cijfertekstletters in een willekeurige volgorde en in kleine letters geschreven. Nu spraken de 2 correspondenten een letter met elkaar af, bijvoorbeeld de letter s. Om een bericht om te zetten in geheimschrift moet de letter s uit de binnenste ring tegen een willekeurige letter van de buitenste ring worden gezet, bijvoorbeeld tegen de F. De hoofdletter F wordt dan als eerste letter opgeschreven, het sein voor de ontvanger dat de s tegen de F is geplaatst. Daarna worden de letters van het bericht – de hoofdletters van de buitenste ring – vervangen door de kleine letters op de binnenste ring die er tegenaan staan.

Na een paar woorden zo te hebben omgezet, verdraaide Alberti de ring echter weer een slag. Als nu de s tegen de D kwam te staan schreef hij eerst weer de hoofdletter D op en ging daarna verder met het omzetten van de letters volgens de nieuwe stand van de twee ringen.
De positie van de binnenste ring veranderde zo voor één bericht diverse malen van stand. Deze poly-alfabetische vervanging was natuurlijk veel moeilijker te kraken dan de tot dusver gebruikte mono-alfabetische vervanging.
Alberti maakte het voor de krakers van zijn geheimschriften nog moeilijker door op de buitenste ring ook de cijfers 1 t/m 4 te plaatsen. Deze gebruikte hij voor een lijst van veel voorkomende woorden die in code gezet waren in getallen van 11 tot 4444. Deze getallen zette hij dan weer om in letters met behulp van de cijferschijf,

Bijvoorbeeld: OVERMORGEN = 341
als de afgesproken letter s tegen de M aanstaat wordt 341 mrp.

Dit geraffineerde gebruik van de cijferschijf werd echter daarna door niemand nagevolgd. Alberti was de enige die codes nòg eens in cijfer zette. Door zijn uitvinding van de cijferschijf kwam de cryptologie van het westen voor het eerst op een hoger niveau te staan dan die van de Arabische wereld. Alberti wordt dan ook wel de 'vader van de moderne cryptologie' genoemd.



## Monoalfabetische vervanging

**is een vervangingssysteem waarbij elke letter van het alfabet door een vaste andere letter wordt vervangen.**

## Polyalfabetische vervanging

**is een systeem waarmee voor de vervanging van elk deel van een bericht, of zelfs voor elke letter een ander alfabet wordt gebruikt.**

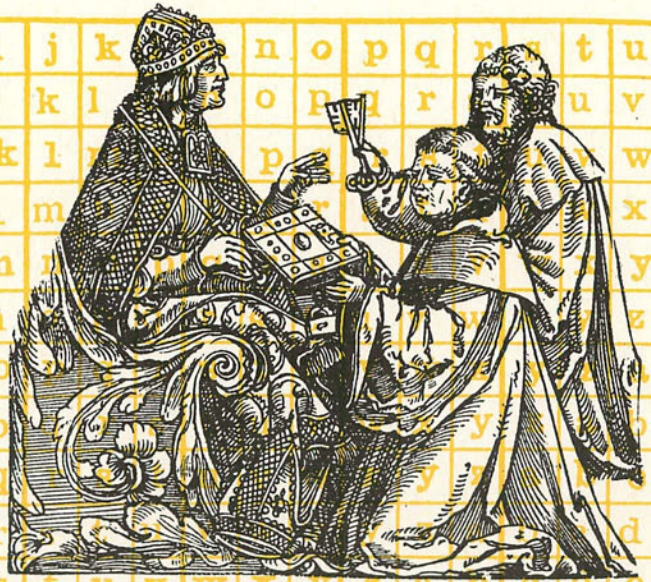


## Sleutelwoord

**Rond 1600 in Rome waren leden van de familie Argenti de belangrijkste cryptanalisten van de pausen. Matteo Argenti schreef een handboek voor cryptologie met daarin de beste nomenclaturen van de Renaissance.
De Argenti's waren de eersten, die een sleutelwoord toevoegden aan een cijferalfabet. Het sleutelwoord gooit zo de voorspelbare volgorde van de letters door elkaar. Bij het sleutelwoord 'crypto', bijvoorbeeld, worden de letters van het alfabet als volgt vervangen:**

C R Y P T O A B C D E enz.
1 2 3 4 5 6 7 8 9 10 11 enz.

**Het sleutelwoord is vast en moet ook aan de ontvanger van het bericht bekend zijn. Het verdient de voorkeur een woord te nemen waarvan de letters op verspreid liggende plaatsen in het alfabet staan, zodat de rest van de letters zoveel mogelijk van plaats verandert.**



*Trithemius biedt zijn Polygraphia aan Keizer Maximiliaan aan.*

# De Polygraphia van Trithemius

a Deus
b Creator
c Conditor
d Opifex
e Dominus
f Dominator
g Consolator
h Arbiter
i Iudex
k Illuminator
l Illustrator
m Rector
n Rex

*De Ave Maria - codelijst van Trithemius.*

Het eerste gedrukte boek over geheimschrift verscheen in 1518. Het werd geschreven door Johannes Trithemius, een beroemd geleerde in zijn tijd. Hij was al op 22-jarige leeftijd abt van een klooster in het Duitse Spannheim en schreef in 1499 een serie boeken onder de titel 'Steganographia', wat uit het Grieks afkomstig is en 'bedekt schrift' betekent. Hij behandelt daarin wel enige vervangingssystemen, maar een groot deel van het boek gaat over magische praktijken, waardoor deze boeken op de Index – de lijst met verboden verboden boeken van de kerk – werden geplaatst. Om zijn naam te zuiveren schreef Trithemius in 1506 een boek in zes delen onder de titel 'Polygraphia', dat alleen over cryptologie gaat, alsof hij daarmee wilde aantonen dat het hem daar ook met de 'Stenganographia' om te doen was geweest. De titel 'Polygraphia' geeft de veelvoud van schrijfwijzen aan, die in het boek behandeld worden. Het grootste deel van het boek wordt echter in beslag genomen door zijn systeem van codelijsten, waarmee letters en cijfers vervangen kunnen worden door woorden die samen een onschuldig lijkend gebed kunnen vormen, bijvoorbeeld het 'Ave Maria'.

Daarnaast staan in 'Polygraphia' cijferalfabetten in het Arabisch en in het Ethiopisch, algaritmische en magische tekens, tekens van de Franken en de Noormannen en de eerste gedrukte versie van een Romeins kortschrift-systeem: de 'Tiroonse noten', een voorloper van ons huidige steno.

In 1518, anderhalf jaar na de dood van Trithemius, verscheen de 'Polygraphia' voor het eerst in gedrukte vorm. De titelpagina laat een houtsnede zien, waarschijnlijk van de hand van een leerling van Albrecht Dürer, waarop Trithemius voor keizer Maximiliaan knielt en hem het boek aanbiedt. Het boek zit op slot zit om het geheime karakter ervan te benadrukken, maar de sleutel wordt erbij gegeven.

## De Tabula Recta

Het belangrijkste geheimschriftsysteem van Trithemius, dat hij in 1506 in zijn boek 'Polygraphia' behandelt, is de polyalfabetische vervanging met behulp van de 'tabula recta', de vierkante tabel.

De eerste letter van het om te zetten bericht wordt vervangen door de letter die eronder staat op de tweede regel, de tweede letter door die uit de derde regel, enzovoort. Zo wordt bijvoorbeeld EEN omgezet in FGQ.

Dit veranderen van alfabet na iedere letter was al weer een stap verder – en dus ingewikkelder om te ontcijferen – dan het gebruik van de cijferschijf van Alberti, die pas na iedere drie woorden de schijf van stand verwisselde. Later werden de mogelijkheden van de 'tabula recta' door anderen verder uitgewerkt.

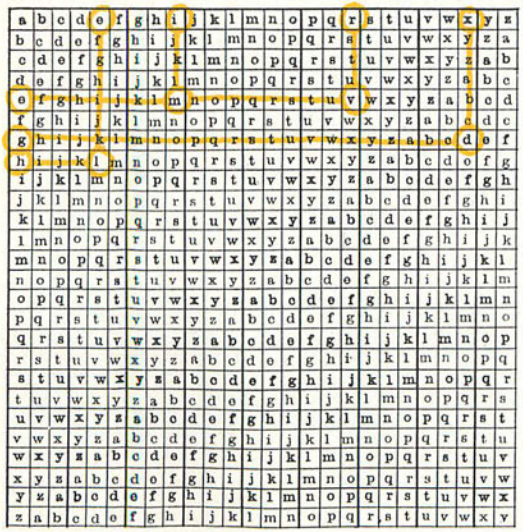
# Belaso's Sleutel

In 1553 verscheen er een boekje met de titel 'het cijfer van de heer Giovan Batista Belaso'. Er is weinig bekend van deze uit Brescia afkomstige man, maar voor de cryptologie vond hij een belangrijke toepassing van de tabula recta van Trithemius: hij combineerde het gebruik ervan met het gebruik van een vast sleutelwoord of een vaste sleutelzin. Hij stelde voor een gemakkelijk te onthouden sleutel te nemen. De letters van het bericht plaatst men dan letter voor letter onder de letters van het sleutelwoord.

Bijvoorbeeld:
de sleutel is: GEHEIMSCHRIFT
en de boodschap is: X REIST NU NAAR Z.
De letters van de boodschap worden onder de letters van de sleutel geplaatst:

G E H E I M S C H R I F T
X R E I S T N U N A A R Z

Elke letter van de klare tekst wordt nu met behulp van de tabula recta vervangen door de letter die er recht onder staat op de regel van de corresponderende sleutelletter. Voor de letter X gaat men vanaf de letter X op de bovenste regel van de tabula recta loodrecht naar beneden tot op de horizontale regel die vooraan links met een G begint. Op die kruising ligt de letter D. D is dus de geheimschriftletter voor X. De gehele boodschap wordt zo: D V L M ... enz.



Door deze eenvoudige toevoeging van Belaso aan de polyalfabetische omzetting van Trithemius werd het systeem van de tabula recta veel flexibeler en daardoor moeilijker te kraken. Gezanten en ambassadeurs konden hun eigen individuele sleutel hebben, maar toch allemaal met de tabula recta werken. Ook bij verlies of ontdekking van een sleutel kon er gemakkelijk een nieuwe worden ingesteld, zonder direkt een heel nieuw geheimschriftsysteem moest worden ingevoerd.

*Cijferschijf van Porta*

# Porta

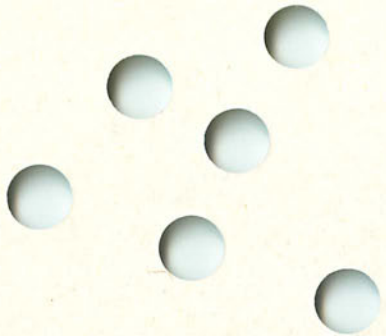


In 1563 verscheen een ander voor de ontwikkeling van de moderne cryptologie belangrijk boek: 'De furtivis literarum notis' van de toen 28-jarige Giovanni Batista Porta uit Napels.

Daarin verdeelde hij crypto-systemen in 3 soorten:
- verplaatsing van letters in een alfabet (transpositie)
- verandering van de vorm van een letter (vervanging door symbolen)
- vervanging door een letter uit een ander alfabet (of een cijfer).

Hij spoorde ook aan zoveel mogelijk synoniemen te gebruiken en 'schrijffouten' te maken in plaats van dubbele letters te gebruiken om frequentieanalyse bij het ontcijferen te bemoeilijken. 'Het is beter voor een schrijver voor dom te worden aangezien, dan te moeten boeten voor het ontdekken van plannen', schreef hij.
Op het gebied van de polyalfabetische geheimschriften legde Porta de basis voor het moderne idee van de polyalfabetische vervanging dat in de 20e eeuwse chiffreermachines is toegepast: hij combineerde het onregelmatige alfabet van de cijferschijf van Alberti en de methode van de letter-voor letter-vervanging met behulp van de tabula recta van Trithemius met Belaso's gebruik van de gemakkelijk te verwisselen sleutel.

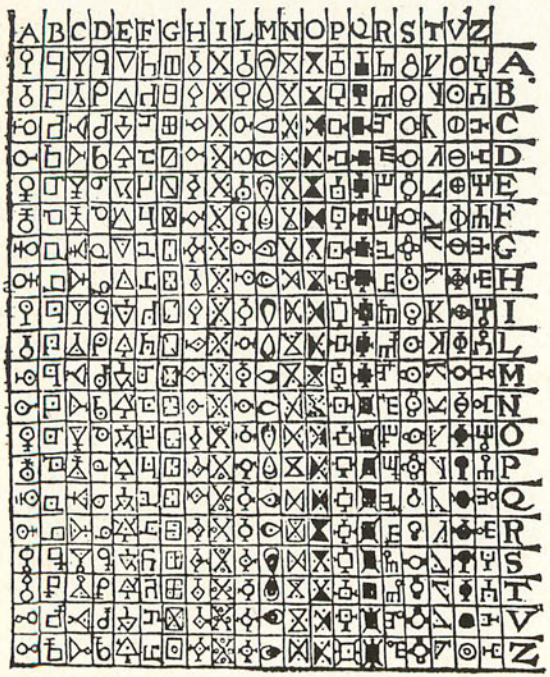
Hij raadde aan de volgorde van de letters in de tabula recta volledig willekeurig te nemen, 'als iedere letter maar aan bod komt', en voor de sleutel volkomen irrelevante woorden te kiezen, want 'des te verder zij verwijderd zijn van algemene kennis, des te meer veiligheid zij geven aan het geschrevene'.



Terwijl in zijn tijd de meeste methodes voor cryptanalyse nog alleen toepasbaar waren op geheimschriften waarbij de woordindeling gehandhaafd was, gaf Porta al een methode waarmee een monoalfabetisch geheimschrift zonder een woordindeling, of met een valse woordindeling ontcijferd kon worden.



Zijn belangrijkste bijdrage aan de geschiedenis van de cryptanalyse is echter zijn methode voor het oplossen van het tot dan toe grootste probleem van een ontcijferaar: het kraken van een polyalfabetisch geheimschrift. De herdruk uit 1593 van zijn boek door een Londense drukker onder de titel 'De occultis literarum notis' bevat zelfs beknopte tabellen die de weg laten zien die een cryptanalist moet volgen bij het ontcijferen van een gegeven cryptogram.




## Het Rooster van Cardano

**Girolamo Cardano, in 1501 in Milaan geboren, was de uitvinder van een geheimschriftrooster, dat zijn naam kreeg. Dit rooster werd gemaakt van een stevig materiaal waarin verspreid over het oppervlak rechthoekige gaten werden uitgesneden ter hoogte van één regel maar van verschillende lengte. Dit rooster werd op een blanco vel gelegd, waarna de woorden van de boodschap in de gaten werden geschreven, soms een heel woord per gat, soms een letter of een lettergreep. Daarna werd het rooster van het papier gehaald, en de rest van het vel werd volgeschreven, zo dat er een onschuldig ogende tekst ontstond. Cardano raadde aan deze tekst nog eens over te schrijven om eventuele verschillen in handschrift, die anders argwaan zouden kunnen wekken, uit te sluiten. De ontvanger van de brief diende daarna nog slechts zo'n zelfde rooster over de tekst heen te leggen om de boodschap te kunnen lezen. Het grootste nadeel van deze methode is natuurlijk, dat vreemde zinsconstructies al het belangrijkste van het geheim konden verklappen, namelijk dàt er een geheim in de brief verborgen zat. Toch heeft een aantal landen in de 16e en 17e eeuw het rooster van Cardano gebruikt voor hun diplomatieke correspondentie.**

*Tussen de vele geheimschriftsystemen en draaibare cijferschijven, die Porta in zijn boek presenteert, staat ook het eerste systeem in de geschiedenis van de cryptologie, waarin twee letters samen vervangen worden door één symbool: het zogenaamde bigrafische systeem.*

# De Boodschap zelf als Sleutel

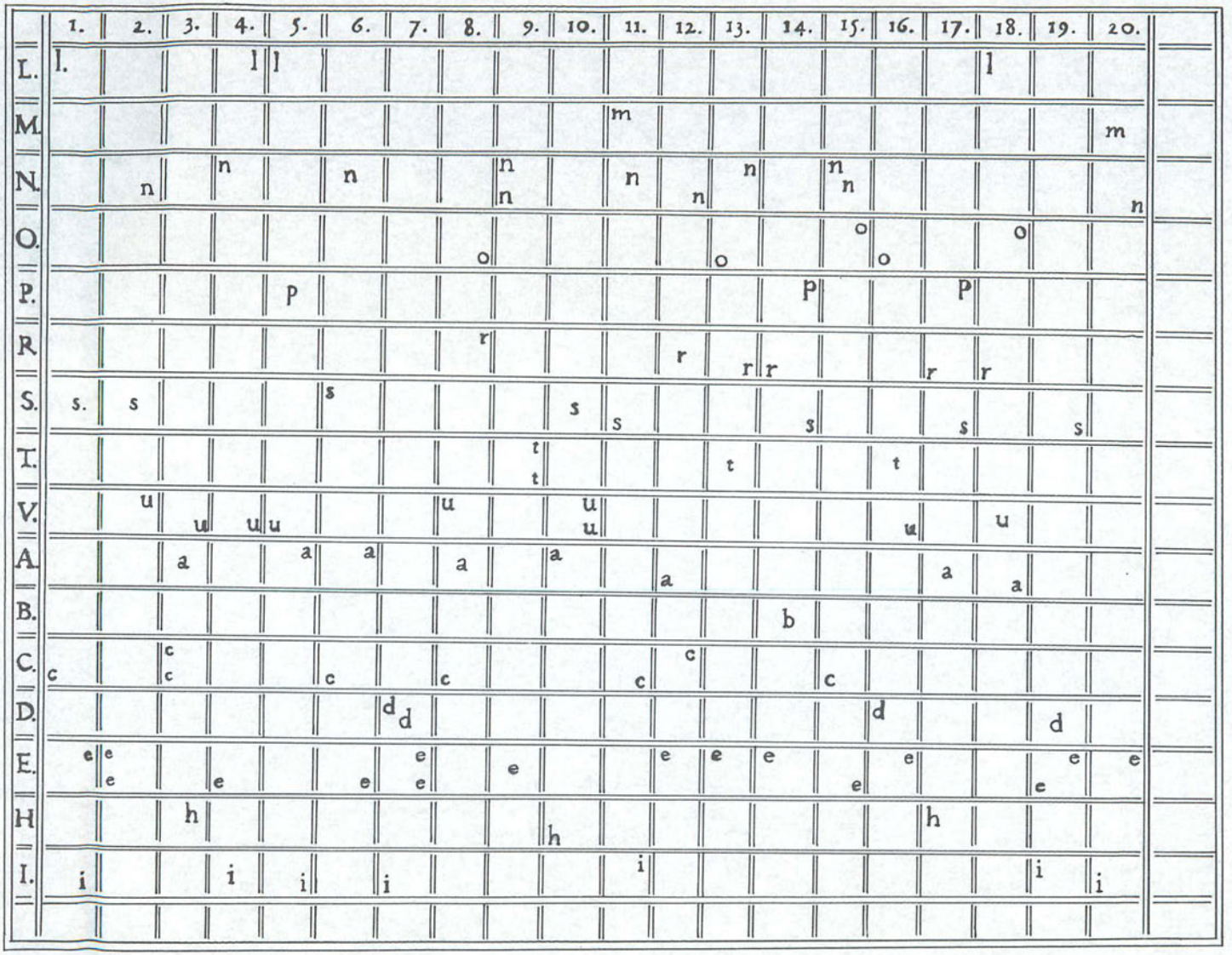
Cardano heeft nòg een belangrijke uitvinding gedaan voor de ontwikkeling van de cryptologie: het gebruik van de boodschap zelf als sleutel in combinatie met de tabula recta. Het idee op zich was goed, maar Cardano zelf paste het verkeerd toe. Hij plaatste boven ieder woord van de klare tekst als sleutel dezelfde letters van de klare tekst steeds van voren af aan beginnend. Het nadeel hiervan was, dat als eenmaal het eerste woord van de klare tekst gevonden was de rest vanzelf volgde, niet alleen voor de ontvanger, maar ook voor de kraker.

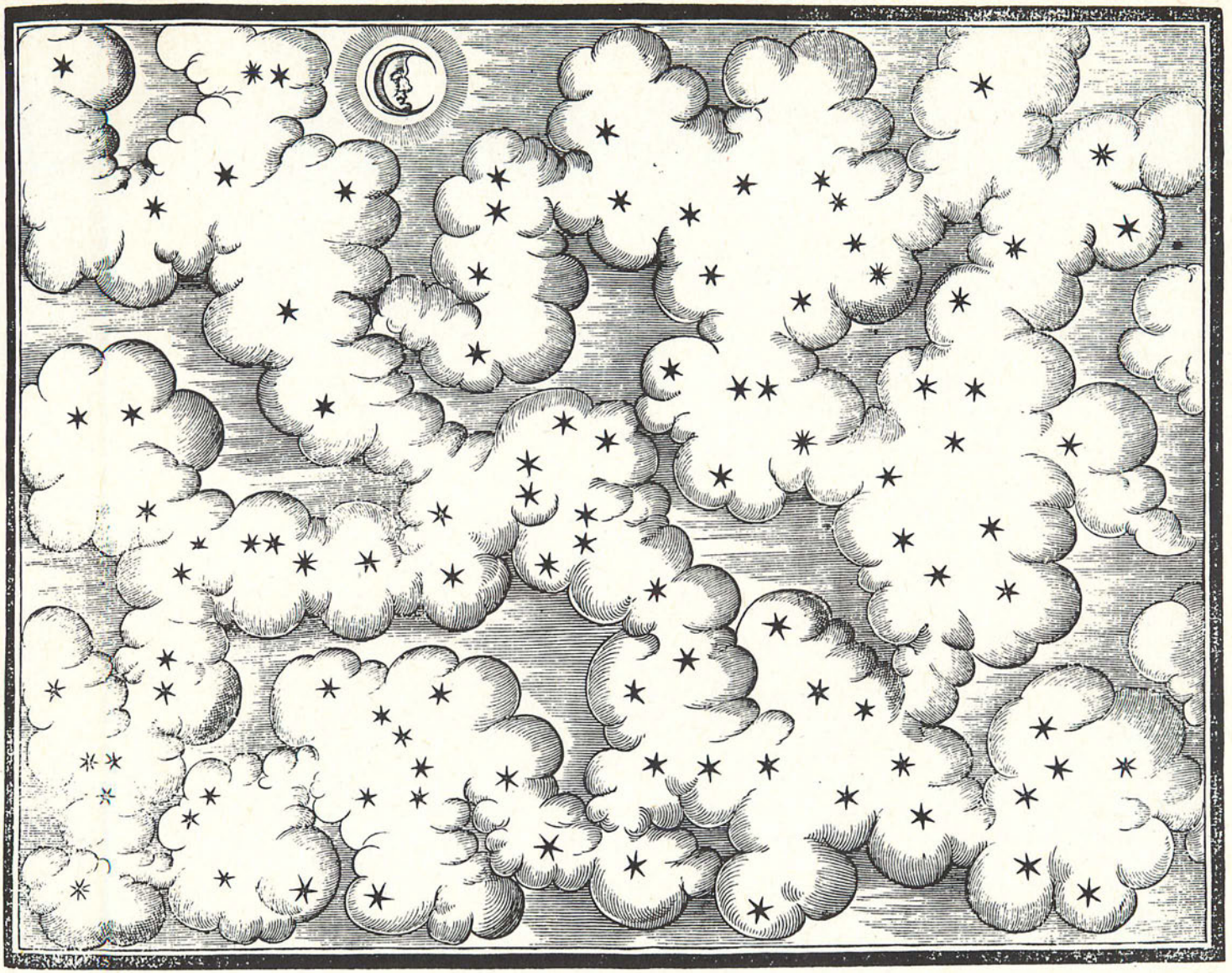
Een tweede systeem dat de boodschap zelf als sleutel gebruikte werd beschreven door Blaise de Vigenère. Dit systeem werkte wel goed.
Hij plaatste voor de boodschap een vaste sleutelletter, die de ontvanger ook kende en die bij ontcijfering met behulp van de tabula recta de eerste letter van de klare tekst opleverde. Deze letter diende weer om de tweede geheimschriftletter te ontcijferen enzovoort. In tegenstelling tot Cardano liet Vigenère de sleuteltekst boven de klare tekst doorlopen, in plaats van bij ieder woord weer van voren af aan te beginnen. Daarna wordt de tekst weer met behulp van een tabula recta vercijferd.

In het voorbeeld hieronder is de D de eerste sleutelletter:

| | |
|---|---|
| vaste sleutel | D A U N O M D E L E T E R N E |
| klare tekst | a u n o m d e l' é t e r n e l |
| geheimschrift | X I A H G U P T M L S H I X T |

Dit systeem werkte prima en is, na in de 19e eeuw opnieuw te zijn uitgevonden, in diverse 20e-eeuwse chiffreermachines toegepast.


1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20.
L.
M.
N.
O.
P.
R.
S.
T.
V.
A.
B.
C.
D.
E.
H.
I.





*Het bovenstaande geheimschrift is een hemel bezaaid met sterren. Het geeft de onderstaande tekst uit psalm 19 (Vigenère hield zich overigens niet helemaal aan deze spelling):*

*Les cieux en chacum lieu*
*La puissance de Dieu*
*Racontent aux humains*
*Ce grand entours épars*
*noncent de toutes parts*
*L'ouvrage de Ses mains*

*(= 'de hemelen vertellen op elke plaats de macht van God aan de mensen: dit grote wijde gewelf verkondigt overal het werk van Zijn handen).*
*Om deze sterrenhemel te kunnen lezen moet er een rooster overheen gelegd worden. Aan de zijkant van het rooster staan de 16 letters van het Latijnse alfabet in een willekeurige volgorde.*
*Langs de bovenkant staan de nummers 1 t/m 20.*
*De sterren kunnen op vijf plaatsen in een hokje van het rooster vallen:*

| | |
|---|---|
| 1 | 2 |
| | 3 |
| 4 | 5 |

*De nummers geven aan in welke volgorde de letters gelezen moeten worden.*
*In een vertikale kolom kunnen dus maar 5 sterren/letters staan. Daarna worden de letters/sterren in de volgende kolom gelezen.*
*Bijv.: De eerste letters zijn 'Les ci' en staan als volgt in de eerste kolom: l ▪, e ▫, s ▪, c ▫, i ▫. Zo kunnen de sterren van alle volgende kolommen ook worden teruggelezen.*

# VIGENÈNERE: 'ALLE DINGEN BEVATTEN EEN CIJFER'

De Fransman Blaise de Vigenère (1523-1596) kwam met cryptologie in aanraking op een diplomatieke reis in Rome. Hij las er de boeken van Trithemius, Belaso, Cardano en Porta en het nooit uitgegeven manuscript van Alberti. Hij ontmoette de cryptologen van het pauselijke hof, werd toegelaten in hun geheime kamers en vertelde later hierover dat hij er de grootvicaris van de Sint Pieter een Turks geheimschrift zag oplossen in zes uur.
Toen hij 47 jaar was gaf hij zijn jaarloon aan de armen van Parijs en trok zich terug om te schrijven. Zijn meest geciteerde boek is de 'Traicté des chiffres', dat hij in 1585 schreef en dat in de twee daaropvolgende jaren twee keer werd herdrukt. 'Alle dingen in de wereld bevatten een cijfer', schrijft hij hierin, 'de hele natuur is grotendeels een cijfer en een geheimschrift. De grote naam en de essentie van God en zijn wonderen, de daden, de projecten, de woorden en het gedrag van de mens – wat zijn ze voor het grootste deel anders dan een cijfer?'
Naast allerlei onderwerpen, zoals de eerste presentatie in Europa van het Japanse schrift, de geheimen van de kabbala en recepten om goud te maken, geeft hij ook uitgebreide informatie op het gebied van geheimschriften. Hij bespreekt vele systemen, zoals het verbergen van een boodschap in een plaatje van een sterrenhemel of een laurierboom.
Veel van de systemen in het boek van Vigenère zijn polyalfabetisch, uitgaande van een tabula recta als die van Trithemius, hoewel Vigenère door elkaar gemengde alfabetten aan de boven- en zijkant van het tableau plaatste.
Toch is zijn naam abusievelijk altijd verbonden gebleven met de tabula recta zònder de gemengde alfabetten boven en opzij van het tableau en in combinatie met slechts een kort vast sleutelwoord, dat aan de schrijver en ontvanger bekend moet zijn en dat steeds herhaald boven de letters van de boodschap geschreven moet worden. Dit systeem staat bekend als 'de Vigenère'.



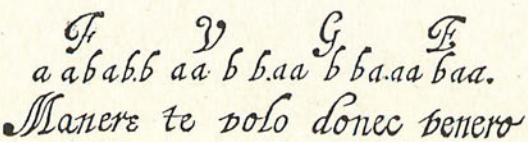
Bijvoorbeeld:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| sleutel | T | IJ | D | T | IJ | D | T | IJ | D | T |
| klare tekst | n | u | i | s | h | e | t | t | ij | d |
| geheimschrift | g | c | r | v | a | m | c | w | b | r |

Vigenère geeft in dit boek echter ook een lijst van diverse sleutel-methoden: woorden, zinnen, dichtregels, de datum van de boodschap, opeenvolgend gebruik van alle alfabetten van de tabula recta en tenslotte zijn versie van de boodschap zelf als sleutel.

Zijn systeem van de tabula recta met gemengde alfabetten in combinatie met bijvoorbeeld de boodschap zelf als sleutel is heel wat moeilijker te breken dan het systeem dat nog steeds zijn naam draagt. Toch is rond dit veel gemakkelijker systeem de legende gegroeid, dat het onkraakbaar zou zijn. Een gerespecteerd blad als 'Scientific American' schreef in 1917 zelfs nog dat het 'impossible of translation' was! De cryptanalisten van zijn tijd wisten natuurlijk wel beter. Zo beschreef Porta bijvoorbeeld hoe hij binnen één uur zo'n geheimschrift kon ontcijferen omdat het de bekende en dus voor de hand liggende spreuk 'omnia vincit amor' (de liefde overwint alles) als sleutel had.

Vigenère gaf aan dat hoe langer de sleutel was, hoe moeilijker het cryptogram te kraken was.
Men wist dus in de renaissance dat een cryptogram, gemaakt met de tabula recta in combinatie met een sleutel, zonder al deze fouten bijna niet te kraken was. Toch bleef men in de drie eeuwen na Porta en Vigenère voornamelijk geheimschriften maken met nomenclaturen (codelijsten), waarschijnlijk, omdat het becijferen en ontcijferen met een nomenclatuur sneller ging en minder kans op fouten gaf. Het gebruik van een tabula recta vergde namelijk nogal wat nauwkeurigheid.
Toch meldt een 17e-eeuws schrijver, dat de Hollanders van tijd tot tijd wel gebruik maakten van polyalfabetische systemen. Ook Napoleon gebruikte voor zijn geheime correspondentie een variant op de Vigenère. Doordat polyalfabetische cryptogrammen verder zo weinig voorkwamen, nam de legende over hun onkraakbaarheid door de eeuwen toe.




**Polyalfabetische cryptogrammen zijn eerder te kraken als:**
- **het geheimschrift de originele woordindeling behoudt**
- **de alfabetten van de tabula recta in de normale letter-volgorde staan**
- **de sleutel een voor de hand liggende term of zin is**
- **de sleutel steeds herhaald wordt.**

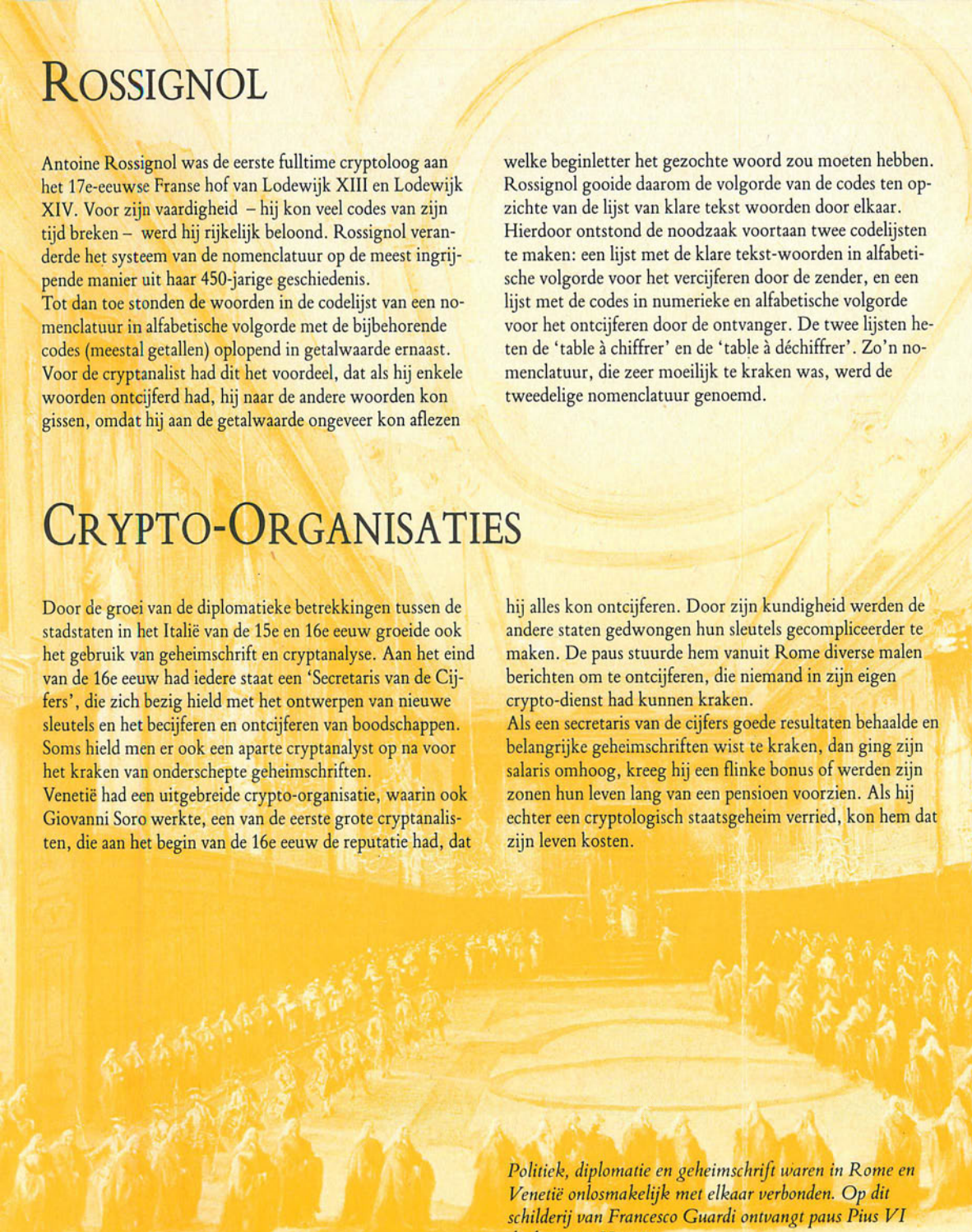
*De Engelsman Sir Francis Bacon (1561 - 1626) vond dat een goed geheimschrift nooit op een geheimschrift mocht lijken. Zijn geheimschrift heeft het uiterlijk van een normale tekst. De code zit echter in het recht of schuin schrijven van de letters.*
*Daartoe bedacht hij een binair alfabet bestaande uit a's en b's. De a staat voor een cursief geschreven letter, de b voor een rechte letter. De te coderen tekst wordt eerst 'vertaald' in groepjes van vijf a's en b's. Dan wordt een onschuldig ogende, willekeurige tekst geschreven in rechte en cursieve letters, volgens het ritme dat de a's en b's aangeven.*

# Rossignol

Antoine Rossignol was de eerste fulltime cryptoloog aan het 17e-eeuwse Franse hof van Lodewijk XIII en Lodewijk XIV. Voor zijn vaardigheid – hij kon veel codes van zijn tijd breken – werd hij rijkelijk beloond. Rossignol veranderde het systeem van de nomenclatuur op de meest ingrijpende manier uit haar 450-jarige geschiedenis.
Tot dan toe stonden de woorden in de codelijst van een nomenclatuur in alfabetische volgorde met de bijbehorende codes (meestal getallen) oplopend in getalwaarde ernaast. Voor de cryptanalist had dit het voordeel, dat als hij enkele woorden ontcijferd had, hij naar de andere woorden kon gissen, omdat hij aan de getalwaarde ongeveer kon aflezen welke beginletter het gezochte woord zou moeten hebben. Rossignol gooide daarom de volgorde van de codes ten opzichte van de lijst van klare tekst woorden door elkaar. Hierdoor ontstond de noodzaak voortaan twee codelijsten te maken: een lijst met de klare tekst-woorden in alfabetische volgorde voor het vercijferen door de zender, en een lijst met de codes in numerieke en alfabetische volgorde voor het ontcijferen door de ontvanger. De twee lijsten heten de 'table à chiffrer' en de 'table à déchiffrer'. Zo'n nomenclatuur, die zeer moeilijk te kraken was, werd de tweedelige nomenclatuur genoemd.

# Crypto-Organisaties

Door de groei van de diplomatieke betrekkingen tussen de stadstaten in het Italië van de 15e en 16e eeuw groeide ook het gebruik van geheimschrift en cryptanalyse. Aan het eind van de 16e eeuw had iedere staat een 'Secretaris van de Cijfers', die zich bezig hield met het ontwerpen van nieuwe sleutels en het becijferen en ontcijferen van boodschappen. Soms hield men er ook een aparte cryptanalyst op na voor het kraken van onderschepte geheimschriften.
Venetië had een uitgebreide crypto-organisatie, waarin ook Giovanni Soro werkte, een van de eerste grote cryptanalisten, die aan het begin van de 16e eeuw de reputatie had, dat hij alles kon ontcijferen. Door zijn kundigheid werden de andere staten gedwongen hun sleutels gecompliceerder te maken. De paus stuurde hem vanuit Rome diverse malen berichten om te ontcijferen, die niemand in zijn eigen crypto-dienst had kunnen kraken.
Als een secretaris van de cijfers goede resultaten behaalde en belangrijke geheimschriften wist te kraken, dan ging zijn salaris omhoog, kreeg hij een flinke bonus of werden zijn zonen hun leven lang van een pensioen voorzien. Als hij echter een cryptologisch staatsgeheim verried, kon hem dat zijn leven kosten.



*Politiek, diplomatie en geheimschrift waren in Rome en Venetië onlosmakelijk met elkaar verbonden. Op dit schilderij van Francesco Guardi ontvangt paus Pius VI de doge van Venetië.*

## Nullen

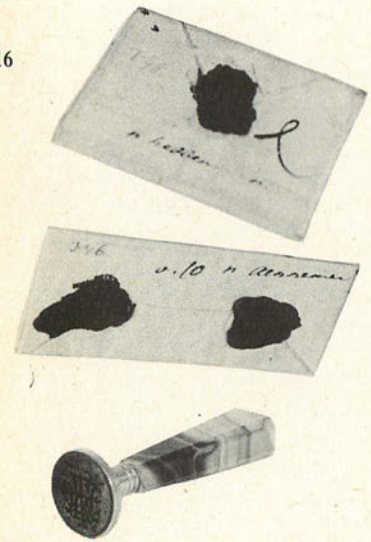
**Om de cryptanalist te misleiden, werden aan een nomenclatuur of een cijferalfabet zogenaamde 'nullen' toegevoegd. Dit zijn letters, cijfers, woorden of andere tekens, die wel in het geheimschrift voorkomen maar in de klare tekst niets betekenen. In de oudste bekende nomenclatuur van paus Clemens VII uit de 14e eeuw kwamen al nullen voor. In latere nomenclaturen konden de lijsten met nullen aan het eind van een codeboek diverse pagina's in beslag nemen.**
**Rond 1483 bedacht men in Milaan de slimme truc van het gebruik van 2 symbolen, die alle tekens, die er in het cryptogram tussen stonden, tot nullen reduceerde.**

| | |
|---|---|
| 13 | **Hy** (*syll.*). |
| 14 | Hygiène, hygiénique. |
| 15 | Hypocrisie. |
| 16 | Hypocrite, hypocritement. |
| 17 | Hypothèque, hypothécaire |
| 18 | Hypothèse. |
| 19 | Dans l'hypothèse. |
| 20 | |
| 21 | |
| 22 | |
| 23 | |
| 24 | |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| 29 | |
| 30 | |
| 31 | |
| 32 | **I** (*lettre*). |
| 33 | Ici. |
| 34 | D'ici. |
| 35 | D'ici à. |
| 36 | Par ici. |
| 37 | Idée. |
| 38 | Idem. |
| 39 | Identique, identiquement. |
| 40 | Identité. |

*Codelijst met 'nullen'.*

# De Zwarte Kamers





*Lakstempel en -zegels.*

In de 16e eeuw kwamen de diplomatieke betrekkingen op gang tussen de europese monarchieën. Men begon incidenteel de post, die van en naar de ambassades ging, te onderscheppen.
In de 17e eeuw werd de post steeds systematischer gecontroleerd en met de aanstelling van Rossignol als eerste fulltime cryptoloog in Frankrijk begint de geschiedenis van de zwarte kamers. Dit was de benaming voor de organisatie, waarin diegenen werkten, die zich de hele dag bezig hielden met het openen, kopiëren en ontcijferen van onderschepte post van andere staten. In de 18e eeuw hadden de meeste landen in Europa zo'n 'cabinet noire' of zwarte kamer.
De zwarte kamer van Wenen was de beste van Europa. Een ploeg van tien man behandelde er tachtig tot honderd brieven per dag die, voordat de post naar de ambassades ging, eerst naar de zwarte kamer werden gebracht. Daar werden de zegels met een kaars losgesmolten, de belangrijke delen werden gekopieerd en vervolgens werden de brieven weer onzichtbaar gesloten, om nog op het normale ochtenduur op de ambassades bezorgd te worden. Daarna werd de gewone post die door dit land heenkwam net zo behandeld en 's middags afgeleverd. Later in de middag kwam dan tenslotte de post binnen die door de ambassades die dag verstuurd werd. Ook deze brieven werden door de zwarte kamer direkt verwerkt, zodat ze nog met de avondpost verzonden konden worden. De kopieën van de brieven werden, indien nodig, vertaald en ontcijferd, waarna de berichten meteen naar het hof werden doorgestuurd.
De cryptanalisten van de Weense zwarte kamer werkten om de week, om ze niet onder de druk waaronder ze moesten werken te laten bezwijken. Hoewel hun loon niet hoog was, konden ze flinke bonussen verdienen met het kraken van belangrijke sleutels. Als de geheime dienst echter door diefstal in het bezit van een sleutel van een ambassade was gekomen werden de cryptanalisten schadeloos gesteld wegens mogelijk gemiste inkomsten.
Maar de grootste stimulans voor de cryptanalisten was waarschijnlijk wel de waardering die zij kregen van hun vorst. Keizer Karel VI kwam persoonlijk de bonussen overhandigen en keizerin Maria Theresia sprak vaak met de leden van de zwarte kamer over hun werk en over de cryptanalytische kennis van andere landen. Zij informeerde bijvoorbeeld of haar eigen ambassadeurs niet al te lang in dezelfde nomenclatuur hadden geschreven en een nieuwe sleutel zouden moeten krijgen.

*Schrijfgarnituur met o.a. briefopener en lakstempel.*

In Engeland was de Post Office verdeeld in de 'Secret Office' voor de buitenlandse post en de 'Private Office' voor de binnenlandse. De Secret Office bestond uit drie kamers, waarvan er in één voortdurend een haardvuur en kaarsen brandden. Ook hier werd de post opengemaakt en zorgvuldig zonder sporen weer gesloten met behulp van nagemaakte zegels.
De Engelse wet voorzag zelfs in machtigingen om in naam van de regering poststukken te laten openen. De post werd als de beste manier gezien om staatsgevaarlijke plannen op het spoor te komen. De Secret Office stuurde kopieën van onderschepte brieven in klare tekst direkt door naar de koning en teksten die in cijferteksten geschreven waren naar de cryptanalisten.

In Nederland werd tussen 1751 en 1803 de buitenlandse politiek vanuit den Haag gevoerd. Hiervandaan werd ook alle buitenlandse post verzonden. In de overige provinciën was er nog geen centraal postbedrijf, totdat Lodewijk Napoleon in 1806 voor de eerste centralisatie van de Nederlandse post zorgde naar Frans voorbeeld.
Het Haagse postkantoor had in de periode van 1751 tot 1803 een zwarte kamer waarvan het bestaan aan slechts enkele beambten bekend was. Dezen moesten er voor zorgen dat het vertrek altijd verwarmd was. Hier werd de post van de Franse en Pruisische ambassadeurs systematisch onderschept en door de secretaris van de cijfers overgeschreven, waarna hij het bericht thuis decodeerde. Tijdens de Franse overheersing werd de hele Nederlandse post door de Franse postkamer gecontroleerd.

Terwijl de Engelse wet de staat machtigde post te onderscheppen en te controleren, erkende de Nederlandse wet het briefgeheim. In de 18e eeuw stond op het verduisteren van een aangetekende brief zelfs de doodstraf.

In Wenen en Parijs werd ook de post van de bevolking zelf gecontroleerd. Dit had tot gevolg, dat de zwarte kamers in deze steden tijdens de revoluties van 1848 door woedende menigtes werden bestormd. Daarmee kwam er een einde aan het tijdperk van de zwarte kamers in Europa.

# De Secretaris van de Cijfers

Aan het eind van de 18e eeuw was er in de 'Republiek van de Verenigde Provinciën', zoals Nederland toen heette, een strijd gaande tussen de 'patriotten' en de 'orangisten', de aanhangers van de stadhouder Willem van Oranje. De 'patriotten' wilden een eind maken aan de macht van de rijke kooplieden en bankiers die Nederland in werkelijkheid bestuurden.

De archieven van de belangrijkste personen uit deze periode zijn rijkelijk voorzien van geschriften in code. Ongetwijfeld omdat brieven in deze burgeroorlog-achtige situatie gemakkelijk onderschept konden worden en men in feite nooit zeker wist wie men kon vertrouwen.

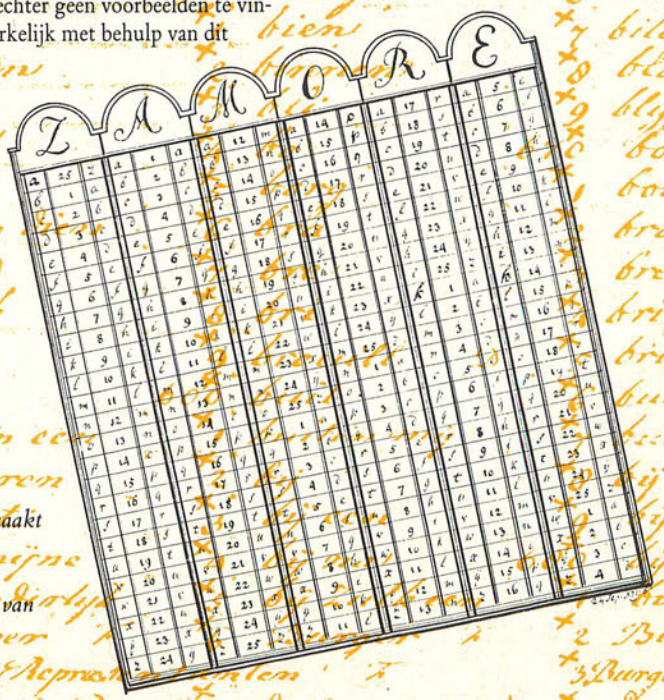
Een heel interessant archief uit deze tijd is dat van de laatste raadspensionaris Laurens Pieter Van de Spiegel, die na de Restauratie in 1787 de hoogste man was onder de stadhouder. In de periode daarvoor, toen hij nog pensionaris van Zeeland was, correspondeerde hij veel in geheimschrift met het hof van de stadhouder, dat uit veiligheidsoverwegingen in Nijmegen zetelde. Veel van de correspondentie van het hof werd in code gevoerd, vooral als het politiek of militair van aard was.

Na de Restauratie, toen Van de Spiegel belast was met de buitenlandse zaken van Holland, gebruikte hij twee geheimschriftsystemen: een nomenclatuur voor zijn correspondentie met de Nederlandse ambassadeurs in het buitenland en een simpeler systeem voor boodschappen aan privé-spionnen en echte vrienden.

De Nederlandse nomenclaturen waren uitgebreide lijsten met duizenden codegroepen. Sinds 1738 werden deze gemaakt door de secretaris van de cijfers, Lyonnet. Toen in 1751 de zwarte kamer werd opgericht, werd de secretaris van de cijfers tevens belast met het ontcijferen van de onderschepte post. Zo schreef Van de Spiegel dat hij honderden gecodeerde brieven per jaar ontving. De zwakte van het diplomatieke geheimschriftgebruik lag niet zozeer in de code die werd gebruikt, als wel in het feit dat men een beroepsontcijferaar in dienst had die politiek onbetrouwbaar of omkoopbaar kon zijn. De secretaris van de cijfers die sinds 1788 onder Van de Spiegel werkte, Croiset – een neef van Lyonnet – was inderdaad niet te vertrouwen omdat hij een aanhanger was van de patriotten. Dit bleek in 1788, toen de Franse ambassadeur zijn brieven niet meer met de gewone post verstuurde maar met een eigen koerier, waarna Croiset ervan werd beschuldigd geheimen aan de Fransen te hebben doorgegeven. Later werd de beschuldiging wel ingetrokken, maar toch bleef men twijfelen aan zijn loyaliteit. Toen Van de Spiegel in 1795 in onderhandelingen verwikkeld was over een wapenstilstand met de Fransen werd Croiset zelfs tijdelijk op non-actief gesteld.

Tijdens de Bataafse Republiek werd de buitenlandse politiek bepaald door de Fransen, waardoor er na 1803 geen post meer door Croiset werd onderschept. Hij trok zich geleidelijk aan terug en werd opgevolgd door Toulon, wiens nomenclatures minder goed waren. Na 1830 waren er in Nederland nog wel enkele nomenclaturen in gebruik, maar door het verdwijnen van Nederland als grote mogendheid, was de buitenlandse politiek niet meer zo belangrijk en nam de kwaliteit van de gebruikte nomenclatures zichtbaar af.

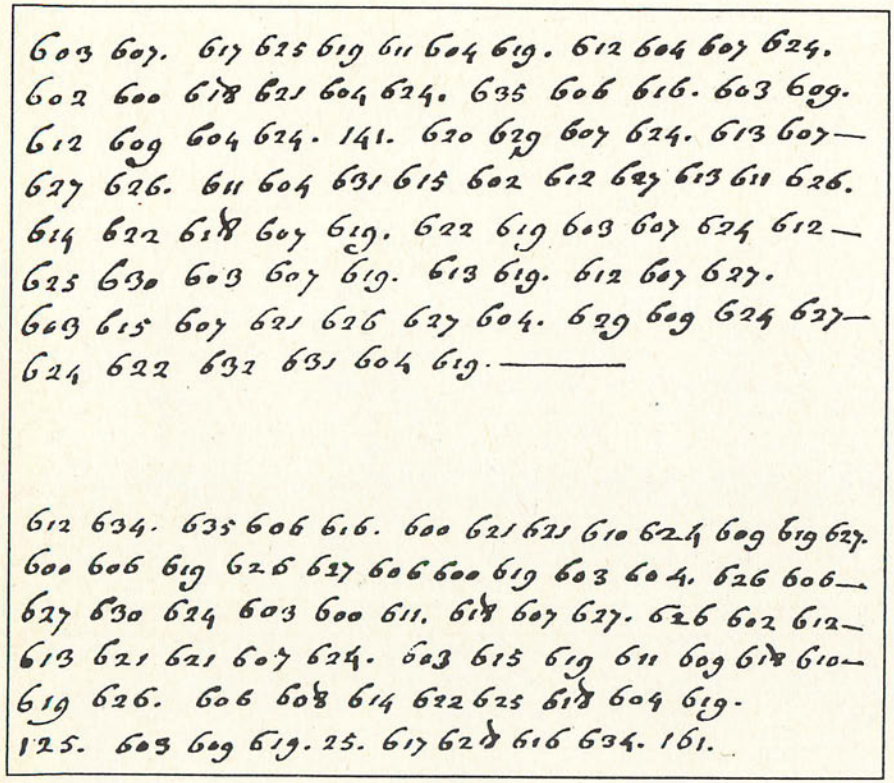
Voor de correspondentie met zijn eigen informanten gebruikte Van de Spiegel geheimschriften die hij zelf maakte. Toen hij door de Bataafse autoriteiten gevangen gehouden werd, vermaakte hij zich zelfs met het maken van een bigrafisch systeem (waarbij twee letters samen door één ander teken worden vervangen) en met met bedenken van diverse variaties van een tabula recta, zoals het mooi uitgevoerde systeem 'ZAMORE', dat werkt als een tabula recta van Vigenère. In zijn archief zijn echter geen voorbeelden te vinden van brieven die daadwerkelijk met behulp van dit systeem zijn gecodeerd.




*In geel: nomenclatuur, gemaakt door Croiset.*

*Het 'ZAMORE'-systeem van Van de Spiegel.*

# Hoe een Bericht Ontcijferd Wordt




*1. Het oorspronkelijke cryptogram.*

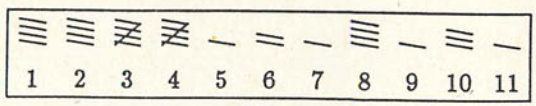
In het archief van raadspensionaris Van de Spiegel in het Rijksarchief in Zuid-Holland bevindt zich een boodschap in code, waarvan zowel datum, plaats als afzender onbekend zijn. In hun onderzoek naar 18e-eeuwse geheimschriften in Nederland voor de Universiteit van Amsterdam hebben de onderzoekers Karl de Leeuw en Hans van der Meer dit bericht als volgt ontcijferd.

Het cryptogram (figuur 1) bestaat grotendeels uit getallen van drie cijfers, waarvan de meeste liggen tussen de 600 en de 635 (zie de frequentietabel van het cryptogram, figuur 2). Het aantal van deze getallen, 36, is zo klein, dat het systeem van een monoalfabetische vervanging met homophones voor de meest frequente letters zeer voor de hand lag. De andere vier getallen zijn dan waarschijnlijk codes voor plaatsnamen of namen van betrokken personen.
Daarna werd de aandacht getrokken door de punten, die in het hele cryptogram tussen de getallen staan en door de strepen, die alleen aan het eind van sommige regels voorkomen. Het lag voor de hand de punten te zien als spaties tussen de woorden en de strepen als verbindingstekens in woorden, die op de volgende regel doorlopen.

| | | | |
|---|---|---|---|
| 25 / | 606 𝍸 / | 616 /// | 626 𝍸 // |
| 125 / | 607 𝍸 𝍸 / | 617 // | 627 𝍸 //// |
| 141 / | 608 / | 618 𝍸 | 628 / |
| 161 / | 609 𝍸 / | 619 𝍸 𝍸 //// | 629 // |
| 600 𝍸 | 610 // | 620 / | 630 // |
| 601 | 611 𝍸 | 621 𝍸 / | 631 // |
| 602 /// | 612 𝍸 // | 622 //// | 632 / |
| 603 𝍸 //// | 613 //// | 623 | 633 |
| 604 𝍸 //// | 614 // | 624 𝍸 𝍸 | 634 // |
| 605 | 615 /// | 625 /// | 635 // |

*2. Frequentietabel van de getallen.*

Dan moest uitgemaakt worden in welke taal het bericht is geschreven. Dat kan het Nederlands zijn, de moedertaal van Van de Spiegel, maar ook het Frans gezien zijn interesse voor de in 1787 naar Frankrijk gevluchte patriotten, die hij in de gaten bleef houden. Figuur 3 laat de in het cryptogram voorkomende woordlengtes zien: 9 van de 27 woorden zijn redelijk lang (met acht of meer letters), wat deed vermoeden dat het bericht in het Nederlands is geschreven. De verdere cryptanalyse is daarop gebaseerd.




*3. Het voorkomen van woorden met een bepaalde lengte.*

Het grootste probleem is altijd het eerste 'gat' in het cryptogram te maken. Hiervoor werden de uitgangen van de langere woorden onderzocht (figuur 4).

| | |
|---|---|
| Laatste getal: | 619 624 626 619 604 619 627 604 611 624 626 619 |
| Eén na laatste getal: | 604 604 611 607 627 604 619 603 600 607 619 604 |

*4. Een aantal laatste getal/een na laatste getal combinaties.*

Het getal 619 blijkt aan het einde van 7 woorden te staan, waardoor het een goede kandidaat is voor de letter N. En

omdat in de uitgang van veel Nederlandse woorden de E voor de N staat, zal 604 ongetwijfeld de E zijn. De combinatie 607-619 komt ook in enkele uitgangen voor, terwijl 607 in 7 woorden op de één-na-laatste plaats staat. Blijkbaar gaat het hier om een homophone en is ook 607 een vervanging voor de E. Zo ontstond het vermoeden dat 624 waarschijnlijk een homophone voor N is, wat later fout bleek te zijn, maar dat hinderde de analyse verder niet.

Toen werden de korte woorden bekeken. De boodschap begint met 603 E. Bijna zeker gaat het hier om het lidwoord DE. En als de eerste conclusies juist waren, dan kon het 14e woord 613 N alleen IN betekenen. Voor de combinatie 612 607 627 zou HET een goede gissing kunnen zijn. Het 10e woord 613 607 627 626 = IET 626 zou dan IETS kunnen zijn.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 606 | | | | | | | | |
| | | | | 607 | | | | | | | | |
| | | | 603 | 609 | | | 612 | 613 | | | | |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 619 | | | | | | | | | | | | |
| 624 | | | | | | 626 | 627 | | | | | |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

*5. Voorlopige vervangingstabel.*

Op dit moment werd er naar de vervangingstabel (figuur 5) gekeken om te zien of er aan de hand van de tot zover gemaakte gissingen al een systeem duidelijk werd. Dit was inderdaad het geval: de waarde van de getallen loopt in dezelfde richting op als de volgorde van de letters van het alfabet. De cryptanalyse zat dus op het juiste spoor. Daarna kon de rest vrij eenvoudig ingevuld worden: IN HET werd uitgebreid tot IN HET DIEPSTE, waardoor zowel de P als een homophone voor de I werden gevonden. Aangezien 621 voor de P stond werd nu duidelijk dat, vanwege het parallel oplopen van de getallen en de letters, 624 niet een homophone voor de N kan zijn. Het lag nu meer voor de hand dat 624 voor de R staat.

Figuur 6 laat de tot zover ontcijferde getallen ingevuld in

D E.617 625 N 611 E N.H E E R.602 600 618 P E R.635 606 616.D E .H E E R.141.620 629 E R.I E T S.611 E 631 I 602 H T I 611 S. 614 622 618 E N.622 N D E R H 625 630 D E N.I N.H E T.D I E P S T E.629 E R T R 622 632 631 E N.

H 634.635 606 616.600 P P 610 R E N T.600 606 N S T 606 600 N D E.S 606 T 630 R D 600 611.618 E T.S 602 H I P P E R.D I N 611 E 618 610 N S.606 608 614 622 625 618 E N.125.D E N.25.617 628 616 634.161.

*6. Tot zover ontcijferde tekst.*

het cryptogram zien, waaruit blijkt, dat de sleutel gevonden is. Andere woorden lieten zich daarna gemakkelijk invullen, zoals ONDERHOUDEN in de eerste zin en SCHIPPER in de tweede. De uiteindelijke sleutel wordt getoond in figuur 7 en het ontcijferde cryptogram in figuur 8.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 600 | | | | | | | | | | | | |
| 606 | | | | 606 | | | | | | | | |
| 608 | | | | 607 | | | | 613 | | | | |
| 610 | | 602 | 603 | 609 | | 611 | 612 | 615 | 617 | 614 | 616 | 618 |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| | 620 | | | | | | 628 | | | | | |
| | 622 | | | | | | 630 | | | | | |
| 619 | 625 | 621 | | 624 | 626 | 627 | 632 | 629 | 631 | | 634 | 635 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

*7. De definitieve sleutel.*

D E.J O N G E N.H E E R.C A M P E R.Z A L.D E.H E E R.141.O V E R.I E T S.G E V I C H T I G S.K O M E N.O N D E R H O U D E N.I N.H E T.D I E P S T E.V E R T R O U W E N.

H Y.Z A L.A P P A R E N T.A A N S T A A N D E.S A T U R D A G.M E T.S C H I P P E R.D I N G E M A N S.A A K O O M E N.125.D E N.25.J U L Y.161.

*8. Het ontcijferde cryptogram.*

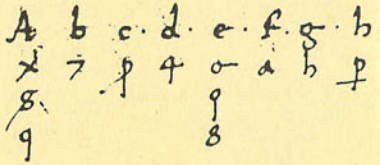
Uit de oplossing maakten de cryptanalisten op dat de sleutel zo simpel is dat het vrijwel zeker niet door de secretaris van de cijfers Croiset is gemaakt. De boodschap zal waarschijnlijk geschreven zijn voordat Van de Spiegel raadspensionaris werd, of anders gemaakt zijn door een van zijn persoonlijke informanten, voor wie hij de code zelf had ontworpen. Nader onderzoek van de brieven van de raadspensionaris wees uit, dat deze sleutel nog in drie andere brieven was gebruikt, die alle geschreven waren in de zomer van 1787 door W. van Citters, een belangrijk edelman uit Van de Spiegels eigen provincie Zeeland. Deze moet dus de schrijver zijn geweest van de ontcijferde boodschap, die nu ook gedateerd kon worden: 25 juli 1787.

Dan restte nog de vraag aan wie de brief is gericht. De naam Dingemans, die van de schipper, is een typisch Zeeuwse naam. In de almanak van Middelburg komt een kapitein 'Dingeman Dingemanse' voor, die iedere vrijdag naar Delft en Den Haag vertrok. Dit is zeker de gezochte schipper, omdat die hoogstwaarschijnlijk terugkeerde op zaterdag, precies de aangekondigde dag van aankomst van de 'jongen heer Camper'. Dit duidt er op dat Van de Spiegel de geadresseerde is, omdat hij in die tijd nog pensionaris van Zeeland was. Hiermee is ook verklaard waarom het bericht in zijn archief gevonden werd.

## Homophones

**De eerste cijferalfabetten vervangen steeds één letter door één andere letter. Later vindt men de meervoudige vervanging uit: voor veelgebruikte letters worden meerdere letters of cijfers ter vervanging neergezet, de homophones, zodat deze letters bij een frequentieanalyse er niet direkt uitspringen.**
**Het oudtse cijferalfabet met meervoudige vervanging dat we kennen is in 1401 gemaakt door de hertog van Mantua, die alleen de klinkers liet voorzien van homophones. Dit bewijst, dat hij nu ook bekend was met cryptanalyse, omdat homophones alleen worden gebruikt als er een vermoeden bestaat dat een ander het geheimschrift zal gaan analyseren.**
**Na 1550, toen ook de codelijsten van de nomenclaturen langer werden, begon men in cijferalfabetten tevens medeklinkers van homophones te voorzien.**





*Homophones voor de A en de E uit een 15e eeuws Italiaans handschrift.*

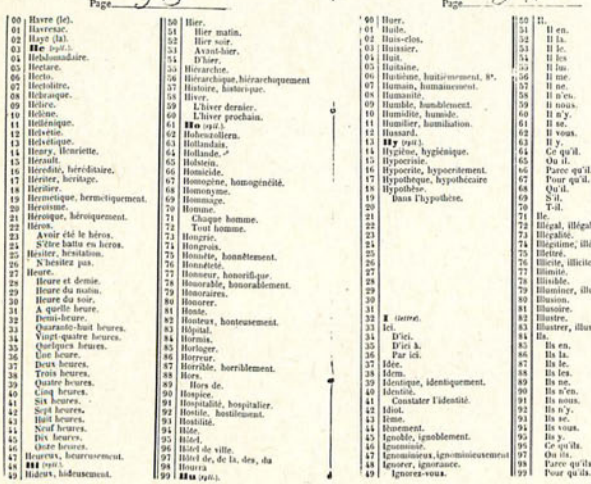
# GEHEIMSCHRIFTGEBRUIK IN DE DIPLOMATIE



In de diplomatieke diensten bedient men zich voor de correspondentie van en naar de ambassades al sinds de 16e eeuw van geheimschrift. Door onder andere het bestaan van de zwarte kamers in de diverse Europese landen was men genoodzaakt diplomatieke geheimen in code te versturen. Eeuwenlang heeft men hiervoor nomenclaturen gebruikt omdat berichten er sneller en zekerder mee te coderen en decoderen waren dan met behulp van een cijferschijf of een tabula recta. Het was daarbij wel van belang de ambassadeurs regelmatig van een nieuwe sleutel te voorzien, want over hoe meer onderschepte gecodeerde brieven van een zelfde nomenclatuur de zwarte kamer van het gastland beschikte, hoe gemakkelijker het werd de sleutel te reconstrueren.

Als in de tweede helft van de 19e eeuw de telegraaf haar intrede doet in de diplomatieke correspondenties, vindt het onderscheppen van diplomatieke berichten niet meer in de zwarte kamers plaats, maar op de telegraafkantoren.

In een brief uit 1852 stelt de gezant in Londen aan het ministerie in Den Haag voor de 'electromagnetische telegraaf' te gebruiken voor zaken, waarin snel bericht moet worden. De dagbladen en de handel gebruikten het al, zo meldt hij. Maar volgens het antwoord van Buitenlandse Zaken was het technisch nog niet mogelijk om in cijfers te seinen. Zodra dit probleem werd opgelost zou het wel interessant zijn.



Page 56

| | |
|---|---|
| 00 | Havre (le). |
| 01 | Haversac. |
| 02 | Hayé (la). |
| 03 | **He** (pp.). |
| 04 | Hebdomadaire. |
| 05 | Hectare. |
| 06 | Hecto. |
| 07 | Hectolitre. |
| 08 | Hectogone. |
| 09 | Hélice. |
| 10 | Hélène. |
| 11 | Hellénique. |
| 12 | Helvétie. |
| 13 | Helvétique. |
| 14 | Henry, Henriette. |
| 15 | Herault. |
| 16 | Hérédité, héréditaire. |
| 17 | Héritier, héritage. |
| 18 | Héritier. |
| 19 | Hermétique, hermétiquement. |
| 20 | Héroïsme. |
| 21 | Héroïque, héroïquement. |
| 22 | Héros. |
| 23 | Avoir été le héros. |
| 24 | S'être battu en héros. |
| 25 | Hésiter, hésitation. |
| 26 | N'hésitez pas. |
| 27 | Heure. |
| 28 | Heure et demie. |
| 29 | Heure du matin. |
| 30 | Heure du soir. |
| 31 | A quelle heure. |
| 32 | Demi-heure. |
| 33 | Quarante-huit heures. |
| 34 | Vingt-quatre heures. |
| 35 | Quelques heures. |
| 36 | Une heure. |
| 37 | Deux heures. |
| 38 | Trois heures. |
| 39 | Quatre heures. |
| 40 | Cinq heures. |
| 41 | Six heures. |
| 42 | Sept heures. |
| 43 | Huit heures. |
| 44 | Neuf heures. |
| 45 | Dix heures. |
| 46 | Onze heures. |
| 47 | Heureux, heureusement. |
| 48 | **Hi** (pp.). |
| 49 | Hideux, hideusement. |
| 50 | Hier. |
| 51 | Hier matin. |
| 52 | Hier soir. |
| 53 | Avant-hier. |
| 54 | D'hier. |
| 55 | Hiérarchie. |
| 56 | Hiérarchique, hiérarchiquement |
| 57 | Histoire, historique. |
| 58 | Hiver. |
| 59 | L'hiver dernier. |
| 60 | L'hiver prochain. |
| 61 | **Ho** (pp.). |
| 62 | Hohenzollern. |
| 63 | Hollandais. |
| 64 | Hollande. |
| 65 | Holstein. |
| 66 | Homicide. |
| 67 | Homogène, homogénéité. |
| 68 | Homonyme. |
| 69 | Hommage. |
| 70 | Homme. |
| 71 | Chaque homme. |
| 72 | Tout homme. |
| 73 | Hongrie. |
| 74 | Hongrois. |
| 75 | Honnête, honnêtement. |
| 76 | Honnêteté. |
| 77 | Honneur, honorifique. |
| 78 | Honorable, honorablement. |
| 79 | Honoraires. |
| 80 | Honorer. |
| 81 | Honte. |
| 82 | Honteux, honteusement. |
| 83 | Hôpital. |
| 84 | Hormis. |
| 85 | Horloger. |
| 86 | Horreur. |
| 87 | Horrible, horriblement. |
| 88 | Hors. |
| 89 | Hors de. |
| 90 | Hospice. |
| 91 | Hospitalité, hospitalier. |
| 92 | Hostile, hostilement. |
| 93 | Hostilité. |
| 94 | Hôte. |
| 95 | Hôtel. |
| 96 | Hôtel de ville. |
| 97 | Hôtel de, de la, des, du |
| 98 | Houra |
| 99 | **Hu** (pp.). |

Page 57

| | |
|---|---|
| 00 | Huer. |
| 01 | Huile. |
| 02 | Huis-clos. |
| 03 | Huissier. |
| 04 | Huit. |
| 05 | Huitaine. |
| 06 | Huitième, huitièmement, 8e. |
| 07 | Humain, humainement. |
| 08 | Humanité. |
| 09 | Humble, humblement. |
| 10 | Humidité, humide. |
| 11 | Humilier, humiliation. |
| 12 | Hussard. |
| 13 | **Hy** (pp.). |
| 14 | Hygiène, hygiénique. |
| 15 | Hypocrisie. |
| 16 | Hypocrite, hypocritement. |
| 17 | Hypothèque, hypothécaire |
| 18 | Hypothèse. |
| 19 | Dans l'hypothèse. |
| 20 | |
| 21 | |
| 22 | |
| 23 | |
| 24 | |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| 29 | |
| 30 | |
| 31 | |
| 32 | **I** (lettre). |
| 33 | Ici. |
| 34 | D'ici. |
| 35 | D'ici à. |
| 36 | Par ici. |
| 37 | Idée. |
| 38 | Idem. |
| 39 | Identique, identiquement. |
| 40 | Identité. |
| 41 | Constater l'identité. |
| 42 | Idiot. |
| 43 | Ième. |
| 44 | Ilement. |
| 45 | Ignoble, ignoblement. |
| 46 | Ignominie. |
| 47 | Ignominieux, ignominieusement. |
| 48 | Ignorer, ignorance. |
| 49 | Ignorez-vous. |
| 50 | Il. |
| 51 | Il en. |
| 52 | Il la. |
| 53 | Il le. |
| 54 | Il les |
| 55 | Il lui. |
| 56 | Il me. |
| 57 | Il ne. |
| 58 | Il n'en. |
| 59 | Il nous. |
| 60 | Il n'y. |
| 61 | Il se. |
| 62 | Il vous. |
| 63 | Il y. |
| 64 | Ce qu'il. |
| 65 | Ou il. |
| 66 | Parce qu'il. |
| 67 | Pour qu'il. |
| 68 | Qu'il. |
| 69 | S'il. |
| 70 | T'il. |
| 71 | Ile. |
| 72 | Illégal, illégalement. |
| 73 | Illégalité. |
| 74 | Illégitime, illégitimement. |
| 75 | Illettré. |
| 76 | Illicite, illicitement. |
| 77 | Illimité. |
| 78 | Illisible. |
| 79 | Illuminer, illumination. |
| 80 | Illusion. |
| 81 | Illustre. |
| 82 | Illustrer. |
| 83 | Illustrer, illustration |
| 84 | Ils. |
| 85 | Ils en. |
| 86 | Ils la. |
| 87 | Ils le. |
| 88 | Ils les. |
| 89 | Ils ne. |
| 90 | Ils n'en. |
| 91 | Ils nous. |
| 92 | Ils n'y. |
| 93 | Ils se. |
| 94 | Ils vous. |
| 95 | Ils y. |
| 96 | Ce qu'ils. |
| 97 | Ou ils. |
| 98 | Parce qu'ils. |
| 99 | Pour qu'ils. |

*Codeboekje uit de diplomatieke dienst.*

Nadat de zwarte kamers tijdens de opstanden van 1848 waren opgeruimd, ontstond er in Wenen toch langzaamaan weer een goed georganiseerd departement voor het onderscheppen en ontcijferen van diplomatieke berichten. In Nederland was dit niet het geval. Dat blijkt ook uit een brief uit 1908 van de gezant uit Lissabon aan Buitenlandse Zaken in Den Haag, waarin hij opmerkt dat het cijferboekje gewoon in de handel verkrijgbaar is en er te weinig wijzigingen binnen de diplomatieke dienst plaats hebben, waardoor de codes te lang hetzelfde blijven. Het departement in Wenen zou volgens hem goed geschoold personeel hebben en over een uitgebreide lijst beschikken van voorkomende cijfercodes. Hij beklaagt zich erover, dat andere landen een goed georganiseerde cijferdienst hebben, terwijl Nederland alleen zo'n simpel boekje heeft.

## Klagende gezanten

In het Algemeen Rijksarchief zijn talrijke voorbeelden te vinden van gecodeerde correspondentie van en naar het ministerie.
Iedere gezant en ambassadeur beschikte over een cijferboekje waarin de te hanteren codelijst stond met alle pagina's voorzien van een nummer. De code achter het te coderen woord gaf, in combinatie met het nummer van de pagina waarop dit woord in het cijferboekje stond, de te hanteren code.

De cijferboekjes werden regelmatig vernieuwd, van andere paginanummers voorzien of aangevuld met nieuwe woorden of namen. De nieuwe code werd dan door Buitenlandse Zaken naar alle ambassades verstuurd met de opdracht om per omgaande een telegram terug te zenden met 'uw ... ontvangen', waarin het aantal boekjes moest worden ingevuld. De oude cijferstaten dienden daarna te worden verbrand. Na ontvangst van het telegram op Buitenlandse Zaken ging de nieuwe code in. Men beschikte over een 'geheim cijfer' voor geheime berichten en over een 'gewoon cijfer' voor het inkorten van telegrafisch te versturen berichten.
Tussen de diplomatieke correspondentie in het Rijksarchief bevinden zich veel klachten van diplomaten over fouten in de gecodeerde post en over de lengte van de gehanteerde codes. Men vindt vaak, dat de codes korter zouden moeten zijn, om de hoge kosten voor de telegrammen te kunnen drukken, en sluit er dan suggesties bij in voor een beknoptere codering. Het antwoord van het ministerie luidt steevast dat die nieuwe systemen nog meer risico op fouten met

zich mee brengen en de ontcijferaars daardoor meer tijd kosten. De gezant uit Peking antwoordt hierop bijvoorbeeld dat de 200 gulden die hij aan de laatste twee telegrammen moest besteden beslist opwegen tegen dat extra werk en dat de Nederlandse belastingbetaler dat zeker met hem eens zou zijn.

Sinds het eind van de 30-er jaren is in de diplomatieke diensten de nomenclatuur grotendeels vervangen door codeermachines.

*Bericht van de Nederlandse consul in Calcutta over de door de Engelsen gebruikte codering.*

CONSULAAT-GENERAAL DER NEDERLANDEN

CODE 2E EN 3E UITGAVE
BENTLEY'S CODE
IN GEBRUIK.
TELEGRAFISCH ADRES: TUNELESS

Simla "Beverley"

CALCUTTA, 11 September 1937
P.1. CLIVE BUILDINGS.

PER K.L.M.-PILOOT

(4221)-5166/287 STRIKT GEHEIM

ANTWOORD BOVENSTAAND NUMMER AAN TE HALEN

ONDERWERP Cijfering

29 SEP 1937 BUITENL. ZAKEN

10/9 37
1996

Hoewel het wellicht van geen groot belang is, meen ik toch de aandacht erop te moeten vestigen, dat ik er achter ben gekomen, dat naar alle waarschijnlijkheid het geheime cijfer, hetwelk door den Generalen Staf in India gebruikt wordt, dus vermoedelijk ook wel in Engeland, niet rechtstreeks gaat van het Engelsch in het cijfer, doch dat dit telegram eerst wordt overgezet in een vreemde taal (Latijn?), terwijl het daarna in cijfer wordt overgebracht.

De Consul-Generaal,

Visser

No. 132/58.

Lissabon, ten 4 Maart 1908.

Cyfer.

AFGEKOMEN

9 MAART 1908 BUITENL. ZAKEN

Het is Uwer Excellentie zeker niet onbekend, dat in sommige Hoofdsteden bijzondere bureaux belast zyn met de ontcyfering der telegrammen, welke in geheimschrift door de vertegenwoordigers van vreemde Mogendheden verzonden en ontvangen worden.-Zoo staat te Weenen aan het hoofd van het zoogenaamd, „Chiffredepartement" een „Hofrath", die een vry talryk personeel onder zich heeft, dat in de „Chiffreschule" eene speciale opleiding ontvangt.-Dergelyke geheime bureaux bestaan, voorzoover ik heb kunnen nagaan, o.a. ook te Parys en te St. Petersburg.

Wanneer men bedenkt, dat het cyferboekje, dat door Uwer Excellenties Departement gebruikt wordt in den handel verkrygbaar is, dat het in den loop der jaren slechts onbeduidende wyzigingen heeft ondergaan, dat in Oranjeboeken de letterlyke Fransche tekst van cyfertelegrammen gepubliceerd werd, en dat de vertegenwoordigers van eenige buitenlandsche Mogendheden (o.a. Graaf Tattenbach te Tanger en de Russische Gezant te Teheran) onze code bekend hebben, -dan geloof ik, dat men met zekerheid kan aannemen, dat in verschillende hoofdsteden de sleutel van ons cyfer bekend moet zyn.-Wat speciaal Weenen betreft, zoo wordt deze opvat ing bevestigd door Uwer Excellentie

Jonkheer de Marees van Swinderen,
Minister van Buitenlandsche Zaken,
etc.etc.etc. te Haag.

*Brief uit 1908 van de Nederlandse gezant uit Lissabon met klachten over de toegepaste geheimcodes.*

# Bilderdijk en Zijn Schoonzuster

De schrijver Willem Bilderdijk (1756 - 1831) was advocaat te 's-Gravenhage voor arme Oranje-aanhangers. Nadat hij geweigerd had de eed van trouw aan het Fransgezinde bewind af te leggen, werd hij gedwongen het land te verlaten. Hij vestigde zich in Engeland en liet zijn vrouw en kinderen achter. In 1806 keerde hij, inmiddels 'hertrouwd' met Catherina Rebecca Scheickhardt, naar Nederland terug. Hier probeerde hij tevergeefs onder de koningen Lodewijk Napoleon en Willem I een professoraat te krijgen. Tenslotte startte hij in 1816 een cursus als privaatdocent in vaderlandse geschiedenis te Leiden.



Van Bilderdijk – die in allerlei geheimschriftsystemen schreef – zijn acht rebusbrieven bekend, vier van voor de uitwijzing in 1795 en vier uit het jaar van de uitwijzing zelf. Deze brieven en tekeningen zijn door Bilderdijk zonder uitzondering gericht aan de drie jaar oudere zuster van zijn eerste vrouw: Maria Petronella Woesthoven, die gehuwd was met de notaris Samuël Elter te Amsterdam. Zij woonde aan de Keizersgracht bij de hoogbejaarde, rijke erfnicht van de Woesthovens, Adriana van Onna.
De gezusters waren allebei in 1785 getrouwd. Het huwelijk van de Elters was kinderloos gebleven. In het huis van Bilderdijk werd bij herhaling een kind verwacht en geboren; helaas niet altijd behouden.

De eerste brieven – een in rebusvorm en een in spiegelschrift – zijn geschreven in 1791. Toen de Elters op bezoek kwamen verwachte de vrouw van Bilderdijk, Catarina Rebecca, haar vierde kind; het tweede en het derde waren kort na de geboorte gestorven. Louïse, de oudste, was als kind nog altijd alleen, en logeerde vaak bij de Elters, verder was de verhouding tussen de gezinnen afstandelijk. De zwagers respecteerden elkaar, en de zusters hielden door achterdocht en jaloezie hun relatie koel en op zekere afstand.

De brieven uit 1793 zijn van gelijke strekking: Bilderdijk verlangt er naar zijn oudste kind Louïse weer eens te zien, die al weer weken bij de Elters in Amsterdam logeert; een bericht wanneer hij haar zal komen halen; weer een geboortebericht, nu van het vijfde kind, wederom een zoon, die de ouders echter ook al binnen een jaar moeten missen. Dan is inmiddels het huwelijk aan de Haagse Prinsengracht stuk gelopen, een verhouding die door de verbanning in het voorjaar 1795 onherstelbaar wordt.

*Rebus-brief van 22 augustus 1795*

*Zijn herte-lijke(n) groet (grot + e) zendt (z + ent, eend) balling (bal + ling) Bilderdijk (beelden, Bilde + r + dijk) van (wan) Londens (l + honden + s) vrije vest (na)ar Gijsbrechts vissers-wijk.*

Zo gespannen als de relatie met zijn (ex)vrouw in Den Haag was, zo ontspannen was en bleef die met haar zuster, ook tijdens zijn noodgedwongen verblijf in Londen. En weer was zijn oudste kind Louïse daarbij het middelpunt.
De briefwisseling met zijn schoonzus had in de jaren van ballingschap nog een andere reden: Maria Elter - Woesthoven verzamelde en beheerde zijn achtergelaten manuscripten en legde een lijst aan van al zijn geesteskinderen.
De rebusbrieven zijn voor de moderne lezer onoplosbaar, niet alleen vanwege de oudere taal en spelling, maar ook door de gebruikte tekens, die deels teruggrijpen naar het gebruik bij de Rederijkers, drie eeuwen eerder.



*Rebus-brief van 10 augustus 1795*

*'Geliefde zuster. Vele mijner brieven zijn vermist. Met die moogelijk mijn antwoorden aan U. Misleid die gedachte mij niet, neem er geen reden uit, van mij te verdenken, doch meld't, en blijf steeds beminnen Uw broeder*
*Q.N.*
*Yarmouth, August. MDCCXCV'*

*Q.N. is waarschijnlijk te lezen als: Quem Nosti: die gij kent (hebt leren kennen), een veiligheidshalve gebruikte afkoring in tijden van ballingschap.*

*Geliefde (g + onderlijfje, hemdje + d) zuster (sister, Egyptisch muziekinstrument).*
*Velen (violen) mijner (mineur, mijn- of schansgraver) brieven (b + 2 rijven, raspen) zijn (sein-vlag) vermist (ver + mest-hok).*
*Met (metworst) die (dijbeen, dij) mooglijk (m + oog + lijk) mijn (ontploffende mijn) antwoorden (hand + w + oorden, oortjes, oude munten) aan (haan) u.*
*Misleid (priester bij de mis + lei, met spons en griffel + d) die (dij) gedachte (g + D + achten) mij (meiboom, lovertak) niet (net + i).*
*Neem er ( n + emmer) geen (g + 1) reden (r + Hof van Eden, paradijs) uit (afgestrooptre leeuwehuid) van (wan, om kaf van koren te scheiden) mij (meitak) te (thee) verdenken (ver + denneboom + ken) doch (hond) meld (m + ellestok + d) 't en (hen) blijf (b + lijf, tors) steeds (s + theebus + ds) beminnen (b + minnen, zogende voedsters).*
*Uw broeder (broedende kip).*

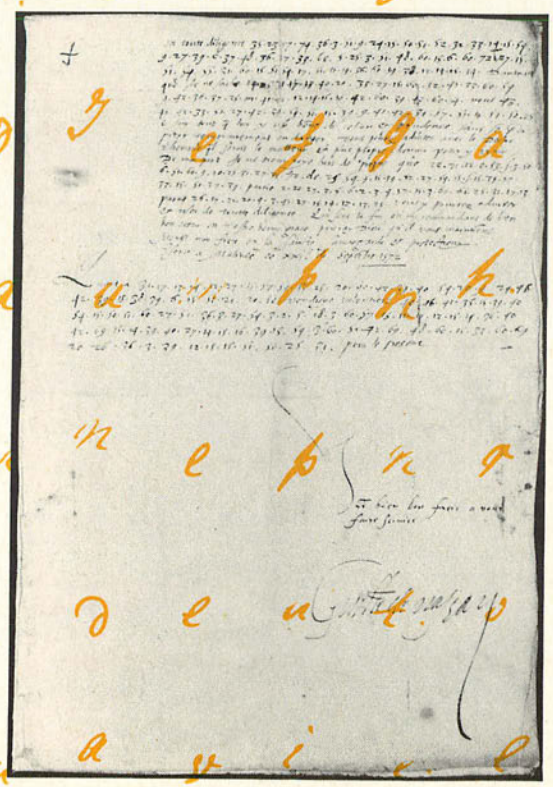
# Vorstelijk Geheimschrift



In het Koninklijk Huis-archief bevinden zich verschillende in code geschreven brieven van en aan leden van de familie van Oranje-Nassau. In de 16e, 17e en 18e eeuw is het gebruik van geheimschrift in het vorstelijk huis zeer gewoon geweest. In het begin gebruikte men vooral een systeem waarbij de letters vervangen werden door tekens en cijfers. Aan het einde van de 17e eeuw kwam een tweedelige nomenclatuur in gebruik, met in het ene codeboek de cijfers en getallen met daarachter de te vervangen woorden en letters en in het andere codeboek de woorden en letters met daarachter de bijbehorende getallen.
Nog later gebruikte men naast codeboeken ook een cijfertabel, waarin voor iedere dag van de week een andere kolom cijfers ter vervanging van de letters stond aangegeven. Aan de datering kon men dan zien welke kolom gebruikt moest worden voor de ontcijfering.

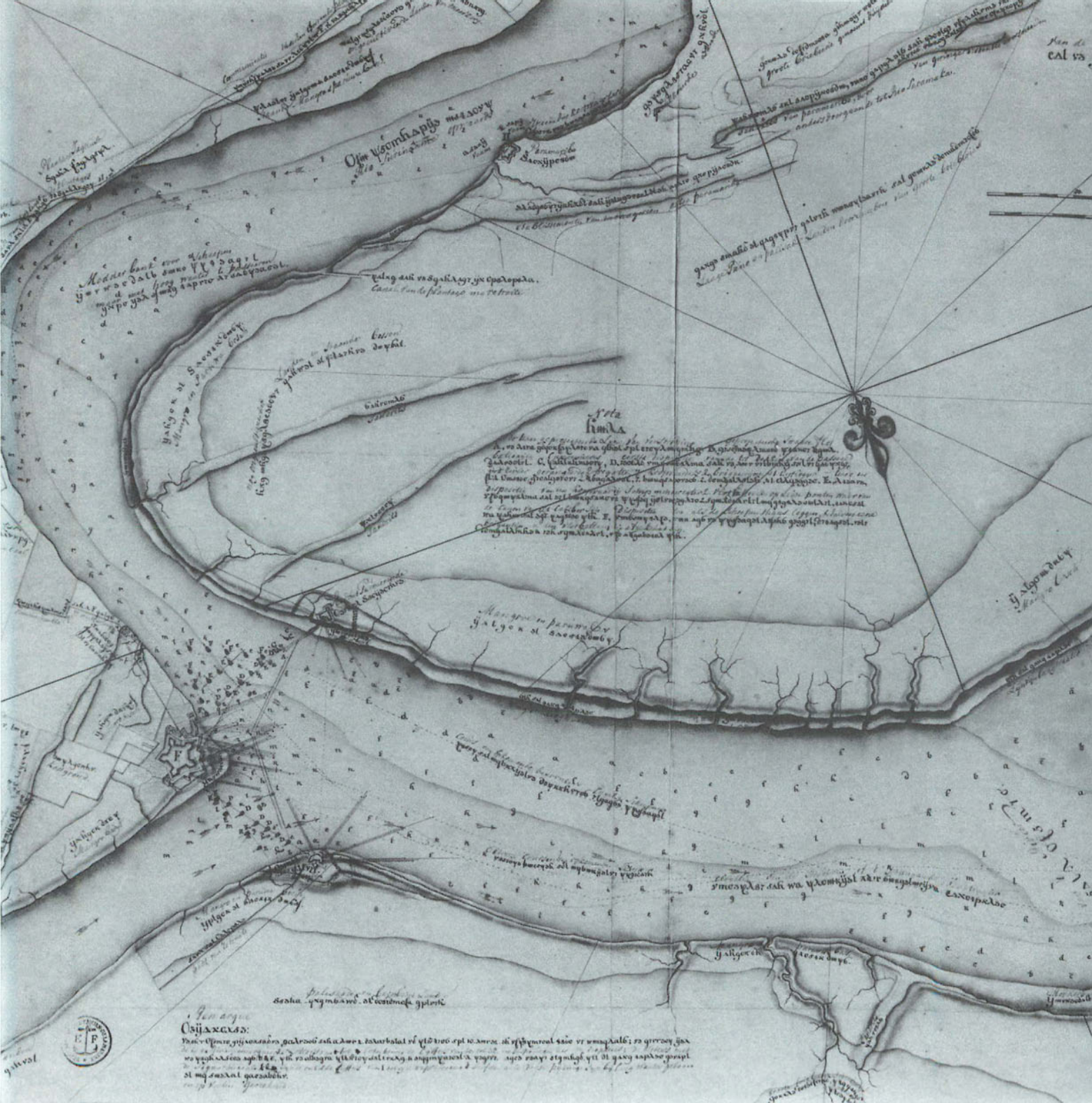
*Rechts:*
*Brief, gedeeltelijk in cijfers, gedateerd 21 september 1572, van Prins Willem I aan zijn broer Jan.*

*Gekleurd:*
*Brief van 21 juni 1800, geschreven met een geheimschriftrooster of Turning Grille, door baron Alexander van Spaendam, de erfprins.*



Toen de Oranjes aan het einde van de 18e eeuw tijdens de Franse overheersing naar Engeland waren uitgeweken, werd er een zeer geheime briefwisseling onderhouden met de trouwe 'orangisten', die een landing van de erfprins in Nederland voorbereidden. In deze briefwisseling komen ook berichten voor in het zogenaamde 'citroenschrift', waarbij het geschrevene pas zichtbaar werd als men er met een lichtzure oplossing overheen streek.

Soms schreef met name prinses Wilhelmina, de echtgenote van Willem V, een brief aan haar zoon over onschuldige zaken. Onderaan de brief zette zij dan een tekentje dat aanduidde dat er een onzichtbaar geheim bericht in de brief stond. Of zij schreef aan haar dochter de datum en plaats van verzending onderaan de brief als er sprake was van een onzichtbaar bericht.
Wilhelmina was goed op de hoogte van geheimschriftsystemen en zij nam veel van de gecodeerde correspondentie van de stadhouder voor haar rekening.
Rond 1800 bediende de erfprins zich nog van een ander systeem: een variatie op het rooster van Cardano, een soort turning grille. In de brieven die hiermee zijn geschreven staan willekeurige letters op gelijke afstand van elkaar in rijen over het blad verdeeld. Om de boodschap te kunnen lezen moest het juiste rooster in verschillende standen over de tekst worden gelegd (zie pagina 25).
In het archief van het Koninklijk Huis bevinden zich van veel brieven die in code zijn verstuurd alleen nog de ontcijferde klare teksten of de minuten, de teksten vóórdat ze in code werden gezet. De originele cryptogrammen werden, nadat ze via omwegen en gevaarlijke tochten op de plaats van bestemming waren aangekomen, na lezing gewoonlijk meteen vernietigd.



# Militair Geheimschrift

Door de geschriften van Griekse en Romeinse schrijvers weten we dat al in de oudheid geheimschrift gebruikt werd voor militaire doeleinden. De geheimschriftsystemen die in de boeken uit de Renaissance en de eeuwen daarna zijn beschreven zullen incidenteel ook wel door legerofficieren zijn gebruikt. Zo geeft het boekje 'De geheime schrijfkunst of briefwisseling' uit 1790 van J.Bronkhorst aanbevelingen voor 'alle legercommandanten, officieren, militairen etc.' De nomenclatuur, die in de diplomatieke wereld zo algemeen gebruikt werd, was echter voor gebruik in het leger niet efficiënt, gezien de omvang van de codeboeken die het niet mogelijk maakte snel een bericht in code te zetten.

In de 19e en 20e eeuw heeft men zich in het leger daarom wel bediend van eenvoudige systemen als de cijferschijf en het roostergeheimschrift, dat afgeleid was van het rooster van Cardano: de 'turning grille'.

Na de uitvinding van de telegrafie in het midden van de 19e eeuw nam het gebruik van geheimschrift voor militaire boodschappen sterk toe vanwege het feit dat de vijand de verzonden berichten ook kon ontvangen.

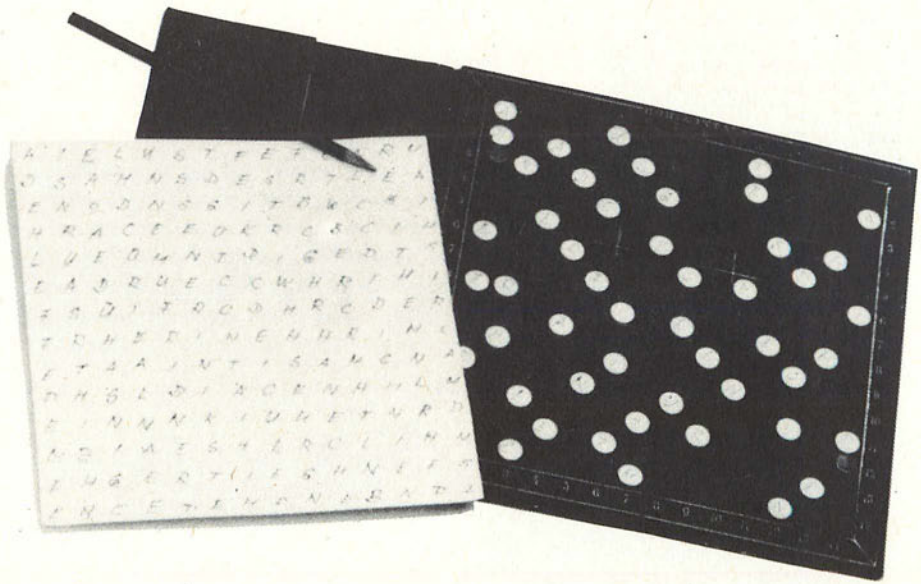
## Kaarten

Militaire stafkaarten zijn eigenlijk nooit in geheimschrift opgesteld, mede omdat de kaarten zelf nooit in onbevoegde handen mochten komen.
Wel worden op burgerkaarten de militaire gebouwen en belangrijke militaire informatie gewoon weggelaten. Dit geeft dan grote witte plekken op de kaart.

Toch bevindt zich in het Rijksarchief een manuscriptkaart van de Surinamerivier uit 1782, getekend door de militair-ingenieur J. Wollant (links). De toelichtende tekst staat zowel in geheimschrift als in een later toegevoegde klare tekst. Wollant heeft een 'generaal plan van defensie' vervaardigd dat, waarschijnlijk vanwege het gevaar van inbeslagname door de Engelsen in geheimschrift is opgesteld. Het gaat hier waarschijnlijk om een polyalfabetische vervanging.

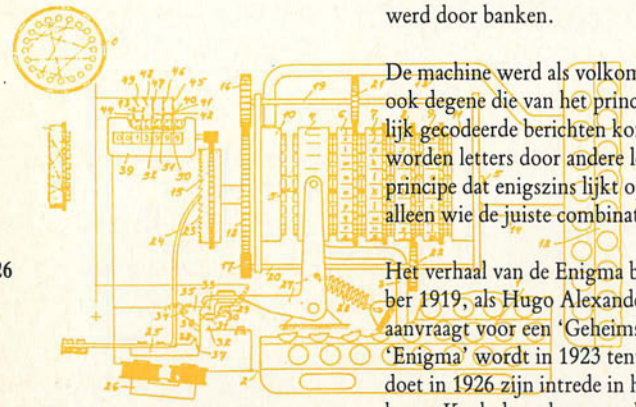
## De Turning Grille

**Dit draaiend rooster bestaat uit een vierkant karton, verdeeld in hokjes. Een kwart van de hokjes moet open zijn, en deze gaten dienen zó gekozen te zijn, dat na 4 keer draaien alle vakjes van het papier eronder één keer te zien zijn geweest. Het rooster wordt op een blanco vel gelegd en de letters van de boodschap worden door de openingen geschreven. Als alle openingen aan de beurt zijn geweest, wordt het rooster een kwart slag gedraaid en worden weer alle openingen van letters voorzien. Dit herhaalt men nog tweemaal. Dan zijn alle plaatsen op het onderliggende vel aan de beurt geweest en staat het volgeschreven met letters, waar geen boodschap uit te halen lijkt. De letters worden dan in een afgesproken volgorde en meestal in groepen van vijf overgeschreven. De ontvanger dient de letters eerst weer in een vierkant terug te plaatsen en eenzelfde rooster te hebben om de tekst terug te lezen. Dit systeem is in de eerste wereldoorlog bij de Duitsers nog in gebruik geweest, als alternatief voor veel te ingewikkelde polyalfabetische systemen.**



# De Enigma





*Interieur van de Enigma*

De Enigma, de geheimschriftmachine die de Duitsers voor en tijdens de Tweede Wereldoorlog gebruikten, stamt uit de jaren twintig. Het was een in de handel verkrijgbare codeermachine die ook in de Verenigde Staten wel gebruikt werd door banken.

De machine werd als volkomen veilig beschouwd, omdat ook degene die van het principe op de hoogte was, onmogelijk gecodeerde berichten kon ontcijferen. Met de Enigma worden letters door andere letters vervangen volgens een principe dat enigszins lijkt op een cijferslot van een koffer: alleen wie de juiste combinatie kent, krijgt de koffer open.

Het verhaal van de Enigma begint in Nederland op 7 oktober 1919, als Hugo Alexander Koch uit Delft het patent aanvraagt voor een 'Geheimschrijfmachine'. De eerste 'Enigma' wordt in 1923 tentoongesteld en het apparaat doet in 1926 zijn intrede in het Duitse leger. In 1927 verkoopt Koch de rechten aan de Duitse uitvinder Arthur Scherbius.

In de Enigma zitten drie tot vijf letterschijven die in verschillende standen kunnen worden gezet. Alleen als begonnen wordt met de schijven in de juiste stand kan een boodschap worden gedecodeerd. De gedachte achter de Enigma is, dat er zoveel verschillende beginstanden mogelijk zijn dat simpelweg uitproberen van alle standen ondoenlijk is – met vijf schijven en wisselende bedradingen in de machine zijn ruim een quadriljoen (1 met 24 nullen) beginstanden mogelijk. Aangezien bovendien elke dag een andere beginstand wordt genomen en de beginstanden gecodeerd worden doorgegeven, lijkt het onmogelijk de machine te 'kraken'.

De Duitsers hadden echter gewaarschuwd moeten zijn. Al in 1932 gaf de Poolse wiskundige Marian Rejewski – als kolonel verbonden aan het Poolse leger – aan hoe het geheimschrift van de Enigma met drie schijven kon worden gedecodeerd. Het enige probleem was dat de methode te lang duurde: tegen de tijd dat de boodschap was ontcijferd, waren de plannen al uitgevoerd.

## De 'Bomba'

Maar de Polen kregen van een spion tevens een deel van de sleutel (de beginstanden) in handen, en daarmee konden de door de Duitsers gebruikte bedradingen worden gereconstrueerd. Hierdoor werd het aantal mogelijkheden tot twee miljard beperkt. Rejewski bouwde een apparaat, de Bomba, dat die mogelijkheden snel kon beproeven – de voorloper van de voorloper van de moderne computer. Het apparaat dankte zijn naam aan het feit dat hij, al rekenend, tikgeluiden maakte als een tijdbom.

In de jaren na 1933 ontcijferde de Poolse inlichtingendienst hiermee talloze Duitse berichten, tot de Duitsers in 1938 een nieuwe Enigma bouwden die vijf schijven had in plaats van drie.
Hier had de Bomba niet van terug.

Dankzij een Poolse mechanicus, die werktekeningen van een voor hem 'eigenaardige machine' Duitsland uit wist te smokkelen, kon Rejewski in 1939 aan zowel de Fransen als de Britten een nagebouwde Enigma ter hand stellen. Na de Duitse inval in Polen, in september 1939, vluchtten Rejewski en zijn medewerkers naar Parijs, waar zij bij de Franse cryptografische dienst gingen werken. Op den duur konden zij de dagsleutel, die iedere dag om middernacht werd gewijzigd, al om vijf over twaalf breken. Hierdoor was het mogelijk de onderschepte, met de Enigma gecodeerde berichten te ontcijferen. Helaas werd de door de Franse en Poolse cryptografen met keihard werken verkregen informatie door de legertop niet altijd even serieus genomen, of werd er laks of te laat op gereageerd.

## Ultra

De Britten intussen, brachten hun Enigma naar Bletchley Park, een dorp op tachtig kilometer ten noorden van Londen – nog steeds hèt telecommunicatiecentrum van de Britse geheime dienst. Daar, onder leiding van Frederick Winterbotham, werkten enkele honderden mensen aan het project 'Ultra'. Deze eerst CX geheten en na 1941 onder de naam 'Ultra' legendarisch geworden 'persoon', was een niet bestaand geheim agent, die door de Britse geheime dienst in 1941 was verzonnen om de werkelijke bron van de gecodeerde berichten, de nagebouwde Enigma, geheim te houden.
In Bletchley Park zaten wiskundigen, linguïsten, musici,

REF. OX/M9B/T531/3

Ko 1444 IN TWO PARTS PART ONE.

ZZZ

KO 1444 £ 1444

KC HC OB 47 £ 47 RJ 32 £ 32 JY 10 £ 10 PK 89 £ 89

CR CNA ON CXA CX YKA YK UO ZAA ZZ FZ OU 77 £ 77 TOA

TO 68 £ 68 WJ 36 £ 36 HX 44 £ 44 LF 30 £ 30 DL 72 £ 72

STR 30 £ 30 STA 59 £ 59 BT 54 £ 54 MI 72 £ 72 XF 91 £ 91

SHR 55 £ 55 FOR ~~FULL~~ CH 23 £ 23 IN TWO PARTS, PART ONE %

WA 472 £ 472

HITLER £ HITLER AT NOUGHT FIVE HOURS TWENTYFIFTH COLON

(ONE) OKW £ OKW RESPONSIBLE TO HITLER £ HITLER FOR FURTHER

CONDUCT OF OPERATIONS AS A WHOLE. (TWO) THE FOLLOWING TO

DIRECT OPERATIONS IN ACCORDANCE WITH INSTRUCTIONS TO BE

ISSUED THROUGH ARMY CHIEF OF STAFF GENERAL KREBBS

WHO IS WITH HITLER £ HITLER. (ABLE) IN SOUTHERN AREA WITH

HELP OF OPERATIONS STAFF BAKER (GENERAL-LEUTNANT WINTER

£ WINTER) COLON ARMY GROUPS SOUTH AND CENTRE, CHARLIE IN

CHARLIE SOUTHWEST £ SOUTHWEST, SOUTHEAST £ SOUTHEAST, AND

WEST £ WEST. (BAKER) IN NORTHERN AREA, DIRECTLY COLON

CHARLIE IN CHARLIE ARMED FORCES NORWAY £ NORWAY AND

JD/CAZ/XE

2614522/4/45

*Links:*
*Generaal Heinz Guderian en medewerkers aan het werk met de Enigma in 1940.*

*Hiernaast:*
*Vertaling van een onderschepte Enigma-brief, waarin Hitler, vijf dagen voor zijn dood, wijzigingen in het Duitse oppercommando aankondigt.*



schakers en typistes in houten barakken bijeen om elke dag weer te proberen de dagcode te breken en die door te geven aan de legerleiding – de ontcijferaars lazen de berichten nooit zelf, alleen de sleutel werd doorgegeven, waarna de geheime dienst de berichten ontcijferde en doorgaf aan Churchill.

De wiskundigen Turing en Newman slaagden er tenslotte in een machine te bouwen die ook de nieuwe Enigma aankon. Een eerste versie was gebaseerd op de vinding van Rejewski en stond dan ook bekend als The Bombe. Enkele geniale grepen van Turing later, in december 1943, kwam de Colossus, een machine waarvan de details nog steeds niet allemaal zijn vrijgegeven. Zelfs het antwoord op de vraag wat nu precies de geniale grepen van Turing waren is nog 'geclassificeerd' materiaal. De Colossus wordt algemeen beschouwd als de eerste echte computer.

De informatie die Ultra verzamelde ( op het hoogtepunt van de oorlog tweeduizend berichten per dag ) kwam van het allerhoogste Duitse niveau – tot aan Hitler toe. Achteraf is het raadselachtig waarom de Duisters steeds vasthielden aan één enkele machine, maar als verklaring wordt gegeven dat een tweede machine in veel opzichten te duur zou zijn geweest en bovendien fouten in de hand zou hebben gewerkt, zodat de betrouwbaarheid van de boodschappen zou afnemen. Daarnaast bleef de Duitse legerleiding overtuigd van de doelmatigheid van de Enigma – zij was meer bevreesd voor ontcijfering door de eigen lagere echelons dan door de vijand. Aan de andere kant konden de Britten – om hun geheim van de beheersing van de Enigma niet prijs te geven – ook niet al te vaak laten blijken dat zij van de vijandelijke plannen op de hoogte waren: sommige Duitse acties werden bewust niet verijdeld.

Toch ging de ontcijfering niet altijd even gemakkelijk. Een van de problemen voor de Britten was dat de onderschepte berichten vaak zwak waren en dus onvolledig of onjuist doorkwamen. Vooral de verwisseling van de V en de U waren berucht. Men probeerde dit te ondervangen door twee versies van elk bericht afzonderlijk te decoderen. Daarnaast deed zich het probleem voor van de hoeveelheid van de onderschepte berichten (soms wel duizenden per dag) en de omvang ervan, waaruit het belangrijkste moest worden geselecteerd. Maar wat had voorrang? Schijnbaar onbelangrijke troepenverplaatsingen konden enorme gevolgen hebben.

Hoewel de Duitsers aan de andere kant ook veel, zo niet alle informatie van de geallieerden konden lezen, staat vast dat de onderschepping van de Duitse plannen een cruciale rol heeft gespeeld in de Tweede Wereldoorlog.

*Marian Rejewski in 1943.*

# HAGELIN: UITVINDER EN MILJONAIR



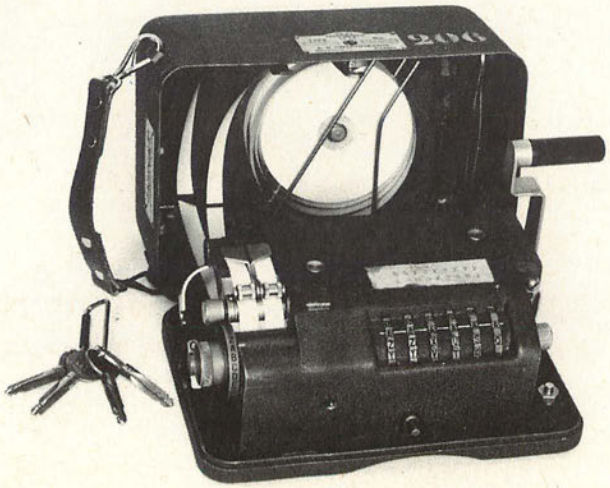
*Boris Hagelin.*

De uitvinder van de Hagelin vercijfermachine was de in 1892 geboren Zweedse uitvinder Boris Caesar Wilhelm Hagelin. In 1923 begon hij voor de 'Aktiebogalet Cryptogaph' te werken, een klein bedrijf dat codeermachines maakte. Twee jaar later ondekte hij dat de Zweedse regering overwoog om de Duitse Enigma te kopen. Daarop vereenvoudigde Hagelin een van de bestaande Zweedse machines, voegde er een sleutelbord en controlelampjes zoals bij de Enigma aan toe, en bood het ontwerp aan het Zweedse leger aan, dat daarop een grote order voor deze apparaten plaatste. Prompt nam Hagelin de leiding van het bedrijf over, dat werd omgedoopt tot 'Aktiebolaget Cryptoteknik'.
Hij zag dat schrijvende vercijfermachines sneller en gemakkelijker te bedienen waren dan machines zoals de Enigma die alleen via lampjes aangaven wat ze ontvingen of verstuurden.
De eerste 'Hagelin' was de B-21, zo groot als een attaché-koffer, 15 kilo zwaar en met een capaciteit van 200 tekens per minuut. Tot 1934 was dit de meest compacte schrijvende vercijfermachine. Toen vroeg het Franse leger aan Hagelin het schijnbaar onmogelijke: een zakformaat vercijfermachine, die de cijfertekst zou kunnen printen en die door slechts één man bediend hoefde te worden.
Hagelin kwam met de B-36, een apparaat dat kleiner dan een telefoon-onderstel was, met een gewicht van minder dan drie pond. Hij kreeg het zelfs voor elkaar dat de cijfertekst in vijf lettergroepen en de klare tekst in normale woordlengte werd geprint. Dit ging met een snelheid van 25 letters per minuut. De Fransen gaven in 1935 de order voor 5000 machines, een keerpunt in de tot dan toe wankele financiële situatie van het bedrijf.

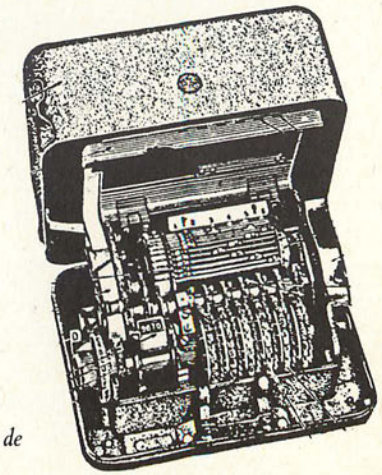
In 1940 vluchtte Hagelin met een gedemonteerde machine, de C-36, en de blauwdrukken naar de Verenigde Staten. Na uitgebreide tests ging het Amerikaanse leger uiteindelijk accoord met de aanschaf van de verbeterde versie, de M-209. In 1942 werden er bij de 'L.C. Smith & Corona Typewriters Company 'in New York ongeveer 400 olijfgroene Hagelins per dag geproduceerd. De totale produktie tijdens de oorlog bedroeg meer dan 140.000 machines. Ironisch genoeg gebruikte het Italiaanse leger ook de Hagelin.
Het cijfer dat de M-209 produceert is polyafabetisch: 26 door elkaar staande alfabetten om 26 letters om te zetten.

Hagelin is de enige die door de cryptografie vermogend is geworden: de rechten liepen in de miljoenen dollars.
In 1944 ging Hagelin – inmiddels multimiljonair – terug naar Zweden, waar hij van een rustig leven dacht te kunnen genieten, omdat de markt voor vercijferingsapparatuur na de oorlog wel ingezakt zou zijn.

Maar de Koude Oorlog en de onafhankelijkheid van veel voormalige koloniën zorgden voor een grotere markt dan ooit tevoren. Omdat de Zweedse wet stategisch belangrijke uitvindingen kan confisceren vertrok Hagelin in 1948 met zijn patenten naar Zug in Zwitserland. Vanwege het fiscale voordeel werd in 1952 daar de hele onderneming, onder de naam Crypto AG, gevestigd.



*De Hagelin MX-3003.*



*Het interieur van de Hagelin M-209.*

# De Ecolex

*De Ecolex.*

De Ecolex IV is een met transistors uitgevoerd vercijferapparaat, gefabriceerd door Philips Usfa, tegenwoordig Philips Crypto in Eindhoven. Het apparaat werd alleen in het Nederlandse leger gebruikt.
De Ecolex werkt met behulp van een telex die de vercijferde tekst verstuurt naar een andere aan een Ecolex gekoppelde telex.
Wanneer een met een Ecolex verzonden bericht wordt onderschept levert dat slechts ruis op, waar geen zinnige tekst van is te maken. Alleen een plotselinge activiteit op de verbindingslijn geeft aan dat er een bericht wordt verzonden.
Bij de Ecolex hoort een dagsleutel, die ieder dag om middernacht wordt veranderd. Deze dagsleutel wordt gebruikt in combinatie met een sleutelband, een ponsband die een schier oneindig aantal combinaties kan produceren. De sleutelband en de dagsleutel vormen samen de sleutel voor het vercijferen.
Bij vroegere Ecolexen was het synchroon lopen van de sleutelbanden nog al eens een probleem. Door het tijdrovende instellen van de banden duurde het een tijd voordat zowel de verzender als de ontvanger aan het vercijferen, respectievelijk ontcijferen konden beginnen. Bij de Ecolex IV is dit probleem opgelost doordat de beide Ecolexen zelf zorgen voor het synchroon lopen van de sleutelband. Niet alleen bespaart dit veel tijd, maar de apparaten worden daardoor ook ongevoeliger voor storingen.

De Ecolex X is een verbeterde versie van de Ecolex IV. Kon men bij de Ecolex IV nog weten dat er activiteit op de verbindingslijn was en dus dat er een bericht overgeseind werd, bij de Ecolex X is er geen verschil merkbaar tussen wel of geen activiteit op de lijn, doordat er een constante ruis op de verbindingslijn wordt geproduceerd, waar eventuele berichten gewoon tussendoor gaan.

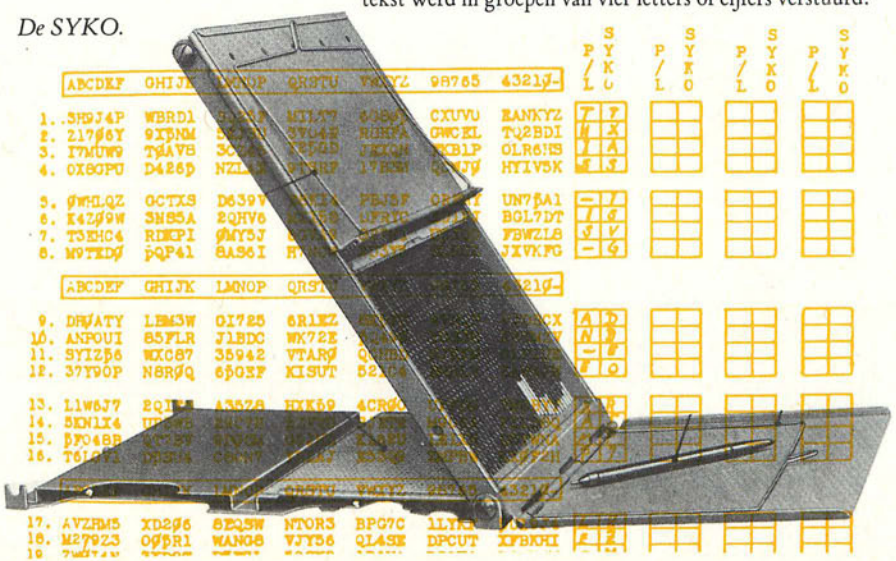
# De SYKO

De SYKO-machine is een codeerapparaat dat na de Tweede Wereldoorloggebruikt werd bij de Nederlandse Luchtmacht voor het vercijferen van berichten over verplaatsingen van vliegtuigen.
De sleutel voor het vercijferen en ontcijferen van een bericht zijn de speciale SYKO-kaarten, waarvan er twee versies bestonden, de militaire- en de burger-kaarten. De burgerkaarten werden gebruikt bij proefvluchten en verplaatsingen van vliegtuigen, de militaire bij gevechts- en verkenningsvluchten. Deze laatste, waarbij geheimhouding moest worden verzekerd, werden alleen uitgereikt aan de officier die met de uitvoering van de opdracht was belast en wel pas tijdens de opdracht. Iedere dag om 15.30 uur werden zowel de militaire- als de burgerkaarten door nieuwe vervangen en telegrafisch doorgeseind.



Het systeem van de SYKO werkt als volgt: het apparaat heeft 32 schuifjes met daarop het alfabet en de cijfers 9 t/m 0.
De kaart met de sleuteltekens schuift men onder de staafjes. Met een speciaal koperen pennetje wordt, te beginnen bij het meest linkse schuifje het pennetje gezet in het tandwiel van de eerste te vercijferen letter of cijfer en naar beneden geschoven tot de pen tegen het frame stuit. Daarna volgt de tweede letter, enzovoort.
De cijfertekst wordt afgelezen op de thans zichtbaar geworden kolom van de SYKO-kaart, hiervoor wordt telkens de eerste letter afgelezen die op de kaart staat direct boven schuif 1, daarna de letter boven schuif 2 enz. De vercijferde tekst werd in groepen van vier letters of cijfers verstuurd.

*De SYKO.*



# Z.O.P

Z.O.P. of Zie Onder Postzegel, kwam in opkomst in 1871 bij de invoering van de briefkaart. Op een briefkaart moest 2,5 cent worden geplakt, terwijl de port voor drukwerk slechts 1 cent bedroeg. Drukwerk mocht in beginsel behalve de naam, beroep en adres van geadresseerde en afzender geen geschreven tekst bevatten. Tot 1925 gold dit ook voor prentbriefkaarten. Indien andere mededelingen, ongeacht van welke aard, op prentbriefkaarten waren aangebracht, werden ze gelijk als briefkaart beschouwd en vervolgens als te laag gefrankeerde briefkaarten beport. Dit soort prentbriefkaarten werd dan in een dienstomslag aan de geadresseerde aangeboden om te voorkomen dat men de prentbriefkaart eerst snel zou lezen en vervolgens zou weigeren de strafport te betalen.

30 Dit tariefsverschil tussen drukwerk en prentbriefkaarten leidde tot een merkwaardige vorm van fraude: de Z.O.P., zie onder postzegel. Men schreef in potlood een bericht onder de postzegel, die losgeweekt diende te worden, en vermeldde elders op de kaart: Z.O.P.

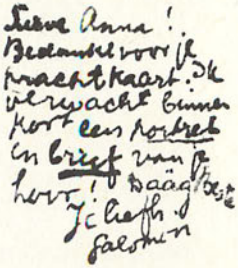
Op 28 oktober 1908 schreef de heer Van Ledden uit Amsterdam een brandbrief aan de Directeur-Generaal der P en T, de heer G. Pop:

Niet wetende of de 'nieuwe wijze tot het ontduiken van port u reeds bekend was', wenste ondergetekende even de aandacht te vestigen op het veelvuldig gebruik van Z.O.P. Hij stelt voor om de postzegels op doorschijnend papier te gaan drukken: 'opdat deze knoeierij belet worde', maar de gomming van doorschijnend papier leverde al sinds eeuwen problemen op.

Overwogen werd zegels met een lichte achtergrond te produceren, zodat de onder de postzegel geschreven tekst zou doorschijnen. Ook zou de tekst gemakkelijk op te sporen zijn door met een penseel benzine op de postzegel aan te brengen, waardoor de postzegel doorzichtig werd. Nog vele andere oplossingen passeerden de revue, maar al met al bleek er niet veel aan te doen.

Het grote aantal kaarten met 'mejuffrouw'-adresseringen zou er op kunnen wijzen dat aan het plegen van ZOP-fraude niet alleen het ontduiken van de port ten grondslag lag, maar ook redenen van privacy. Vaak bevatten de teksten onder de postzegel mededelingen die voor niemand anders dan de geadresseerde bestemd waren. Zo staat er onder een postzegel op een kaart uit 1911, die gericht is aan mejuffrouw van Dijk p/a de heer van Dijk (haar vader?): 'Dag lieverd, ik heb uw brief ontvangen en maak u maar niet ongerust want zoals wij het doen kan het nooit geen kwaad lieverd, u vindt het toch ook wel lekker. No. 1'


*Briefkaart met tekst die onder de afgeweekte postzegel tevooirschijn kwam.*
*Onder: de vergrote tekst.*







# POSTZEGELTAAL

## Voorbericht

(VOOR DEN EERSTEN DRUK.)

De Postzegeltaal heeft ten doel om dengenen, die deze taal machtig zijn, door het uiterlijk van den brief datgene kenbaar te maken, wat de inhoud verzwijgt. Om dit doel te bereiken, plakt men de postzegels op de zijde van het adres, in sommige gevallen ook aan de achterzijde, in verschillende standen op. Elke pluats, die de postzegels, zooals uit de volgende bladzijden blijken zal, kunnen innemen, heeft zijne bijzondere beteekenis. Een verdere verklaring of uitleg zal zeker wel overbodig zijn. Ook spreekt het van zelf, dat voor de Postzegeltaal, slechts die zegels gelden, die den brief behoorlijk frankeeren. De liefde is listig, zoo zullen door een voortdurend streven ook weer nieuwe kunstgrepen op dit gebied te voorschijn komen.

Moge het boekje, dat in Duitschland reeds een 23sten druk beleefde, een vriendelijk onthaal vinden!

*DE UITGEVER.*

## Voorbericht

VOOR DEN TWEEDEN DRUK.

Uit het feit dat binnen 1½ jaar reeds een tweeden druk van dit werkje noodig was, blijkt dat men ook in Nederland met dit boekje zeer ingenomen is.

# Het Patrin: Geheimschrift Van Zigeuners

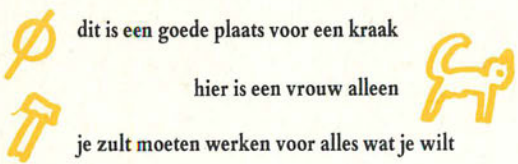
Het Patrin is het symbolenschrift van zigeuners (die eigenlijk Roma heten), dat gebruikt werd en wordt om elkaar inlichtingen te verschaffen. Wanneer een groep in de omgeving van een dorp had vertoefd liet deze een boodschap voor de andere wellicht volgende groepen achter waarin informatie is verstopt over voedsel en handel.

Een mooi voorbeeld hiervan is het volgende.
Een zigeunerin klopt met het verhaal dat ze linnengoed wil verkopen aan bij een boerderij. Daar vraagt ze wat er zich zoal de laatste tijd in het gezin heeft voorgedaan, hoe oud de kinderen zijn, of ze pas ziek zijn geweest, enzovoort. Wanneer ze weggaat krast ze met krijt of houtskool tekens op de muur, die alleen door andere zigeuners begrepen worden. Als er later weer een zigeunerin langskomt, valt het deze niet moeilijk voor helderziende door te gaan.
Ook worden tekens over de mate van vriendelijkheid of vijandigheid van de diverse bewoners op deurposten en muren geschreven. Deze tekens zijn geheim, hoewel een aantal ervan al verscheidene keren is gepubliceerd. Maar omdat de verschillende publikaties elkaar behoorlijk tegen spreken, moet aan de juiste betekenis van de bekend gemaakte tekens zeer getwijfeld worden. Wel geeft het onderstaande rijtje een indruk van het gebruikte systeem.




## Oude Symbolen van Boeven

Of ze tegenwoordig nog gelden is maar de vraag, maar ook boeven en inbrekers hebben hun eigen geheime codes gehad. Zo waren de volgende tekens bekend:



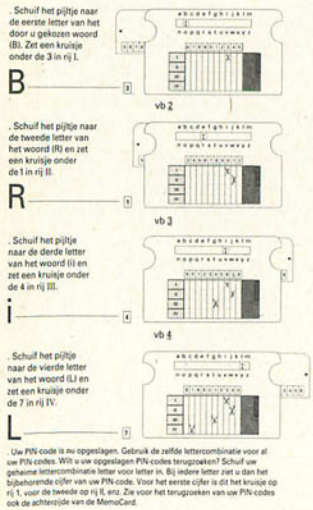

*Rechts: een voorbeeld van 'boevenschrift', afkomstig uit de jaren dertig en werd gevonden op de kapelmuur van een Oostenrijks dorpje dicht bij de grens van Hongarije.*

*De eerste tekening is een papegaai, geschreven in één lijn, wat er op duidt dat het de 'handtekening' is van de dief; het dier geeft aan dat hij bekend staat als 'de papegaai'. De kerk met de sleutel ernaast, kan betekenen dat de kerk vaak niet op slot zit of dat de kerk beroofd gaat worden. Het in doeken gewikkelde kind eronder staat voor kerstavond. Het teken van de drie stenen kwam uit een populaire boerenalmanak en stond voor St. Stephan, die gestenigd was op 26 december. Het totale plaatje betekende:*

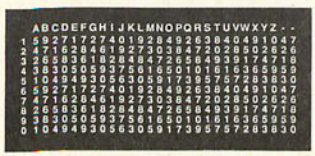
*'De papegaai gaat de kerk beroven op 26 december. Een ieder die hem daarbij wil helpen kan hem hier ontmoeten op kerstavond, dan maken we de afspraken.'*

# Pincodes en Andere Ongemakken






*Handleiding bij de MemoCard*




*Codekaartje van PTT-Telecom.*

Tegenwoordig heeft vrijwel iedereen met cryptografie te maken, en wel in de vorm van de PINcode (Persoonlijk Identificatie Nummer), een getal van vier cijfers, dat bij een betaalpasje hoort.
Aan niemand anders dan de eigenaar is de pincode bekend, ook niet aan de bank. De veiligheid van het systeem staat of valt met de geheimhouding van de pincode door de rekeninghouders.
Maar hoe geheim is de pincode in werkelijkheid?

Er zijn tienduizend getallen van vier cijfers (0000 tot en met 9999); er zijn dus ook tienduizend verschillende pincodes. Maar omdat er veel meer rekeninghouders zijn, hebben duizenden mensen dezelfde pincode. Dat hoeft geen bezwaar te zijn, zolang iedereen zijn pincode maar echt geheim kan houden en als niemand na diefstal van het pasje de kans krijgt alle mogelijke pincodes uit te proberen totdat de juiste gevonden is.

De pincode staat niet op het magneetstripje op het pasje, zoals veel mensen denken. De magneetstrip bevat een hoeveelheid informatie in gecodeerde vorm: rekeningnummer, naam van de klant, enzovoort. Daarnaast bevat de magneetstrip een getal dat correspondeert met de pincode, een soort controlegetal waarbij maar één pincode past. Het kastje dat de pincode 'leest' controleert in werkelijkheid of beide getallen bij elkaar passen.
In principe werkt de controle als volgt:
Stel de optelsom van controlegetal en pincode moet altijd 9999 zijn. Als het controlegetal b voorbeeld 1092 is, dan moet de pincode 8907 zijn, want 1092 + 8907 = 9999. Wordt een ander getal ingetoetst, merkt het apparaat dat de optelling niet klopt, en gaat het rode lampje branden. Zo eenvoudig als in dit voorbeeld gaat het in werkelijkheid niet, maar in grote lijnen komt het hier wel op neer. De controle is niet omkeerbaar: de pincode en het controlegetal leveren opgeteld wel een vaste uitkomst op (a + b = c), maar het controlegetal van de vaste uitkomst afgetrokken levert niet de pincode op (dus niet c - b = a). Magneetstripgegevens en pincode worden samen aan een controletest onderworpen.
Er is een manier om de pincode te achterhalen: met behulp van een los controlekastje, dat niet is gekoppeld aan de hoofdcomputer, net zo vaak proberen tot de code klopt. Met de hand kost het maar een paar uur voordat de pincode bekend is, en met een eraan gekoppelde computer is het karwei in een fractie van een seconde geklaard.

Daarna kan een neppasje worden gemaakt door de magneetstripgegevens te kopiëren en op een blanco pasje te plakken. Het leeghalen van de rekening kan beginnen zonder dat de klant het merkt en zonder dat de bank het merkt! Dat is het zwakke punt van het systeem, want de bank gaat er van uit dat iemand die de juiste pincode kent, de rechtmatige eigenaar is.

## Veilige manieren, andere pasjes

De chipkaart, ook wel 'smart card' (slimme kaart) genoemd is een plastic kaartje waarin zich een klein goudkleurig schijfje bevindt ter grootte van een kwartje. Dit schijfje bevat een chip en een koppelplaatje.
In de chip worden enkele gegevens opgeslagen zoals de identiteit van de toekomstige gebruiker en gegevens over de pincode. Het geheugendeeltje van de chip wordt ontoegankelijk gemaakt voor de controlecomputer doordat de contactpunten in het laatste stadium van de fabricage worden vernietigd. De geheugeninhoud kan door niemand anders dan door de chip zelf worden gelezen. Op deze manier kan de chip bijvoorbeeld een ingetoetste pincode controleren door deze te vergelijken met de pincode die in zijn geheime geheugendeel is opgeslagen. Aan de 'buitenwereld' kan de chip dan doorgeven of de pincode correct is. Bovendien kan de chip zèlf bijhouden hoe vaak er een verkeerde pincode wordt ingetoetst. Bij drie missers achter elkaar maakt de kaart zichzelf onbruikbaar.
Deze kaart is veel veiliger dan de magneetstripkaart, waarbij de beveiliging niet in de kaart zelf zit, maar in de controleapparatuur.


*De chipkaart*

## Wachtwoorden

**Beveiligingssystemen van computers zitten over het algemeen goed in elkaar. Het zwakke punt is meestal de gebruiker.**
**Veel gebruikers nemen wachtwoorden als hun eigen naam, automerk, kenteken of namen van familieleden. Die zijn eenvoudig te raden.**
**Een tip voor een bruikbaar wachtwoord: het serienummer van het eigen horloge; men heeft dat altijd bij zich en het verwijst niet naar iets persoonlijks.**
**Voor de controle van de wachtwoorden bestaat er een wachtwoordenprotocol, een soort vraag- en antwoordspel om te controleren of iemand wel degene is voor wie hij zich uitgeeft.**
**Het wereldrecord wachtwoordenkraken staat sinds augustus 1993 op naam van een speciale computer die 6,4 miljoen vercijferde wachtwoorden per seconde geeft. Dit komt neer op het checken van alle zesletter-woorden binnen een minuut. Wachtwoorden waarin ook cijfers en aparte tekens ($ & % ß * §) zijn verwerkt worden binnen hooguit dertig uur gekraakt. Het vinden van een wachtwoord van acht tekens – tegenwoordig een minimumeis voor een veilig wachtwoord – vergt maximaal drie dagen. Gelukkig kost deze getallenkraker zo veel dat hij nog niet in groten getale beschikbaar is.**

# DES – de Data Encryption Standard

DES is een programma voor het vercijferen en ontcijferen van gegevens. Het door IBM ontwikkelde LUCIFER-systeem werd in een aangepaste en sterk vereenvoudigde vorm in 1977 door de NBS (het Amerikaanse National Bureau of Strandards)in gebruik genomen. Sindsdien is DES op grote schaal in gebruik, niet alleen bij de Amerikaanse overheid, maar ook bij bedrijven en banken over de gehele wereld.
DES is een soort elektronische gehaktmolen die teksten op een ingewikkelde manier door elkaar husselt. De werking van DES is niet geheim, het is zo in de bibliotheek op te zoeken, het is niet moeilijk om er een computerprogramma voor te schrijven en DES kan ook op een chip worden gezet. De veiligheid van DES berust dan ook niet op het geheim van het systeem, maar op de moeilijkheid het te breken.
Het kraken gaat in principe net als bij de pincode: alle mogelijkheden uitproberen totdat de goede is gevonden. Bij de pincode is dat nog wel te doen, omdat er maar 10.000 mogelijkheden zijn. Bij DES is het aantal verschillende sleutels echter veel groter: de sleutel telt 56 bits (56 enen en nullen) die vrij gekozen kunnen worden, dus zijn er $2^{56}$ verschillende mogelijkheden, een getal met zeventien cijfers! Al zou een computer één miljoen sleutels per seconde kunnen testen dan zou deze meer dan duizend jaar nodig hebben voordat hij alle mogelijkheden heeft onderzocht. Dat lijkt ondoenlijk, maar als men naast de gecodeerde tekst een stuk klare tekst heeft en men kan met een aantal parallel gekoppelde computers werken, dan hoeft het maar een paar minuten te duren. Voor grote criminele organisaties die er veel geld voor over hebben is het achterhalen van een DES-sleutel dus niet onmogelijk. Voor zeer kostbare geheimen wordt DES dan ook niet meer aanbevolen.

### De National Security Agency

Naast deze dure mogelijkheid is er – vreest men – nog een manier om het DES-systeem binnen te gaan. De NSA, de 'National Security Agency', de voornaamste codeer- en decodeerafdeling van de Amerikaanse overheid, was verantwoordelijk voor het ontwikkelen van DES. De werkzaamheden van dat instituut, het budget en het aantal personeelsleden zijn geheim, maar men vermoedt dat het bureau twee maal zo groot is als de CIA. Critici beschuldigen de NSA ervan een geheime ingang in het systeem te hebben aangebracht om toegang te kunnen krijgen tot vertrouwlijke informatie en zo als een schaduw-inlichtingendienst te kunnen funktioneren.



# RSA: (Nog) Onkraakbaar

Het in 1978 gepubliceerde RSA is ontworpen door R. Rivest, A. Shamir en L. Adelman, naar wie het systeem is vernoemd. RSA wordt gebruikt bij zeer kostbare geheimen; ook de DES-sleutels worden ermee beveiligd.
Het RSA berust op het principe van modulair machtsverheffen en werkt min of meer als volgt:
Eerst wordt de tekst op een standaard manier in getallen omgezet. Die reeks getallen wordt dan in stukjes met een vaste lengte van ongeveer 100 cijfers verdeeld. Vereenvoudigd gezegd worden de getallen van de tekst versleuteld door ze tot een macht te verheffen en daarna door de sleutel te delen. De rest, die na de deling overblijft, is het resultaat. Met alleen het restgetal van zo'n machtsverheffing is het niet mogelijk om daar door worteltrekking de factoren uit te halen.

Er zijn slimme methoden voor het vercijferen waarmee men binnen enkele seconden resultaat heeft. Maar het ontcijferen werkt anders en is op deze manier onmogelijk. Het probleem schuilt in het feit dat uit het grote RSA-sleutelgetal van tweehonderd cijfers de twee factoren gevist moeten worden, waaruit het is ontstaan. Van het getal 25 bijvoorbeeld, is het eenvoudig in te zien dat 5 x 5 de gezochte factoren zouden moeten zijn. Maar met de huidige stand van de wiskunde en de computertechnologie is het volstrekt ondoenlijk om de twee factoren te vinden waarvan het produkt de gegeven sleutel van tweehonderd cijfers is.
Zolang dit nog geldt, is het RSA een veilig systeem. Het is zeer onwaarschijnlijk dat het binnenkort gekraakt wordt. De National Security Agency werkt het gebruik van RSA en andere veilige systemen tegen, om de mogelijkheid te behouden om in de systemen in te breken.

# Onzichtbare Inkten



Recepten om inkten te maken, waarmee men onzichtbaar kan schrijven waren al in de oudheid in gebruik. Zo zouden de priesters die een orakel lieten spreken ook gebruik hebben gemaakt van boodschappen in onzichtbare inkt. Later gebruikten de alchemisten dit middel om hun geheime formules en recepten door te geven. In onze fantasie worden de onzichtbare inkten dan ook direkt door tovenaars en magische formules omringd. Toch schreef de Egyptische geleerde Qalqashandi al in de 14e eeuw recepten voor geheime inkten juist voor gebruik door secretarissen.
In de Renaisance raadde Alberti aan geheime berichten in onzichtbare inkt te schrijven voor diplomatieke doeleinden. En rond 1600 publiceerde Porta de 'magia naturalis' een serie van twintig boeken vol wetenschappelijke experimenten, waarvan het 15e boek vele recepten bevat voor onzichtbare inkten en trucs als onzichtbaar schrijven op een ei en op de huid van een mens, zodat 'boodschappers gezonden kunnen worden, die noch zullen weten dat ze brieven bij zich hebben, noch erop betrapt kunnen worden'.

In 1777 onderschepte de Engelse zwarte kamer een aantal brieven die waren geschreven in geheime inkt. De chemicus van deze 'black chamber' noteerde dat twee van die brieven, door Amerikanen verstuurd tussen Parijs en Londen, geheel geschreven waren in 'witte inkt'. Op één ervan stond Benjamin Franklin's naam in de kantlijn.

Een reden om een geheim met onzichtbare inkt op te schrijven kan zijn dat codes en de meeste geheimschriften direkt onthullen dàt het om een geheim gaat. Als zo'n brief in handen valt van de tegenpartij zal men de brief, indien deze onontcijferbaar blijkt, liever vernietigen dan doorsturen. Een onschuldig eindje 'wit' papier onder aan een 'normale' brief wekt echter geen argwaan.

In diverse jaargangen van het wetenschappelijke blad 'De Natuur' staan aan het eind van de 19e eeuw recepten en vragen van lezers over zogenaamde 'sympathetische inkten'. In een van die artikelen, 'Eenvoudige proeven op chemisch gebied', door dr. A.J.C. Snijders wordt o.a. het recept gegeven van een zeer verdunde oplossing van het zout cobaltchloruur, dat lichtrose schrijft, bij opdroging verdwijnt, bij verwarming weer blauw opkomt en bij afkoeling weer onzichtbaar wordt. Het artikel eindigt met een uitleg van de term 'sympathetisch': 'Overigens schijnt deze vloeistof wel eens gediend te hebben voor een geheime correspondentie tusschen verliefde personen en daarvan zou dus de naam "Sympathetische inkt" afkomstig zijn'.

Er zijn vele recepten in omloop geweest van vloeistoffen die te gebruiken zijn als onzichtbare inkt. De ingrediënten variëren van huis-, tuin- en keukenmiddeltjes (als melk, zeep, ui en citoen) tot gevaarlijkere chemische oplossingen (als zwavelzuur, ammoniak en zilvernitraat). Het schrift wordt over het algemeen weer zichtbaar gemaakt door het papier te verwarmen of in water te dompelen, al naar gelang de oplossing die men heeft gebruikt. De werking van de 'zwavelzuur- en kopersulfaatmethode' komt wel heel alchemistisch over: 'schrijf met dezen "inkt" het bericht en je correspondent hoeft het dan slechts boven een geopend ammoniakfleschje te houden om het in hemelsblauw te voorschijn te doen komen'.

Tegenwoordig bestaan er uv-pennen, waarmee boeken of kostbare spullen kunnen worden gemarkeerd. Onder een uv-lamp of een hoogtezon wordt de tekst weer zichtbaar.

# 'Ontcijfer'

In 1981 kreeg Warren Holland, verbonden aan de Technische Universiteit van Virginia een lumineus idee om veel geld te verdienen: hij loofde een prijs uit voor het kraken van een door hem gecodeerde tekst.
Hiervoor nam hij een van zijn lievelingsgedichten, E.E. Cummings' 'A Poet's Advice', en koos als sleutel het zesde hoofdstuk van Carl Sagans boek 'Cosmos'. Hij nummerde de beginletters van de opeenvolgende woorden, te beginnen met het woord 'first' in een citaat aan het begin van het uitgekozen hoofdstuk. Tenslotte verving hij de letters in 'A Poet's Advice' door de zo verkregen getallen.
Hij liet de gecodeerde tekst op een legpuzzel afdrukken, zodat er een puzzel in een puzzel ontstond en loofde een prijs uit van f. 200.000 voor degene die voor eind maart 1985 de oplossing wist te vinden.
Van de puzzel, die onder de naam 'Ontcijfer' op de markt kwam, werden meer dan een kwart miljoen exemplaren verkocht.

Onder de velen die zich ten doel hadden gesteld Holland's cryptogram op te lossen was Alan Sherman, een docent aan het Massachusets Institute of Technology. Tijdens zijn colleges over cryptologie ging hij met zes van zijn studenten de uitdaging aan. Zij gebruikten een computersysteem waarbij de gebruiker een potentiële sleuteltekst intypt en waarbij de computer vervolgens allerlei methoden uitvoert voor het toekennen van getallen aan die tekst. Deze methoden worden vervolgens op de codetekst uitgeprobeerd om er een Engelse boodschap uit te construeren.
Het succes van dit systeem hing af van het intypen van de juiste sleuteltekst.
Holland had zelf al een paar cryptische hints gegeven om de puzzelaars op weg te helpen: '3,19' en 'Zou het u helpen als u wist dat het met een C begon?'. 3 en 19 zijn de vercijferde plaatsen in het alfabet van de initialen van Carl Sagan. De tweede hint sloeg op 'Cosmos'.

Toen na een aantal maanden nog niemand de puzzel had opgelost opende Holland een speciaal telefoonnummer met daarop verdere hints. Begin maart 1985 – een paar weken voor de deadline – liet hij doorschemeren dat de sleutel een reeks eerste letters was uit het zesde hoofdstuk van Cosmos. De groep Sherman concludeerde dat er onvoldoende zinnen of regels in het hoofdstuk voorkwamen, dus dat het wel de eerste letters van woorden moesten zijn. Ook de strategie om te beginnen bij 'first' werd door hen bedacht. Het hoofdstuk werd in het programma ingetypt, maar zonder resultaat. Sherman c.s. hadden echter een aantal afkortingen genummerd, die door Holland waren overgeslagen.
Op 27 maart ontwikkelden zij een handige methode om gedeeltelijke overeenkomsten tussen het cryptogram en de sleuteltekst vast te stellen. Zo konden ze complicaties in de nummering van de sleuteltekst omzeilen. Op 29 maart construeerde computer een tekstfragment dat de juiste frequentieanalyse tentoonspreidde. Daarna kon de tekst compleet worden gemaakt en kwam Cummings' gedicht tevoorschijn.
Echter, toen zij de prijs dachten te kunnen claimen, hadden zij over het hoofd gezien dat de laatste inzenddag niet de laatste dag van maart was, maar de laatste werkdag!

## Voor wie eens niets te doen heeft

volgt hieronder tot slot nog een tekst in code. Na alle informatie over cryptosystemen moet het niet moeilijk zijn dit geheimschrift te kraken. De sleutel ligt in uw handen!

19-48-1-13-131-35-63-
5-69-33-138-18-6-31-
12-84-9-23-37-54-49-
189-40-42-55-249-36-
52-62-56-401-41-295-
45-60-107-50-72-2-43-
61-156-65-91-136-
340-4-89-330-68-98-
111-112-157-8-71-76-
340-363-81-94-167-
107-83-98-145-131-7-
149-342-191-324-87-
90-30-36-31-144-151-
102-158-249-340-301-
302-209-66-311-299-
92-160-207-64-352-
401-21-70-3-384-213-
295-14-97-299-107-
78-22-383-16-176-
340-120-180-77-185-
198-405-295-127-205-
432-105-215-24-118-
242-80-27-221-123-
221-230-84-104-129-
233-250-258-255-67-
439-458-599-330-39-
364-409-273-117-260-
133-266-47-599-85-
268-663-467-421-280-
363-294-378-417-418-
96-306-309-308-73-
485-503-615-495-101-
321-139-316-500-116-
202-320-20-446-509-
79-449-615-121-335-
29-337-441-413-328-
75-347-182-143-457-
201-226-350-95-108-
359-717-520-361-381-
130-219-114-351-135-
511-518-634-150-497-
220-226-388-390-717-
166-529-551-595-100-
419-615-588-423-340-
171-109-499-571-254-
615-516-594-427-521-
434-531-153-128-445-
159-461-464-264-172-
486-572-241-576-712-
269-103-574-589-548-
178-490-665-512-685-
86-537-348-367-721-
592-708-561-720-25-
628-737-113-573-712-
607-613-152-193-340-
155-3-707-110-163-
202-737-165-586-374-
400-596-107-136-115-
236-597-620-432-134-
662-131-205-688-424-
28-628-138-239-257-
226-189-187-638-640-
599-175-1-295-13-
330-192-674-683-48-
32-151-615-257-137-
184-655-438-3-33-
330-729-154-259-34-
37-717-38-676-363-
253-299-31-624-42-
57-52-287-55-44-56-
495-19-500-452-46-
684-509-170-60-521-
275-413-342-460-202-
72-531-91-190-98-
107-339-181-111-324-
713-156-714-195-341-
226-218-51-35-183-
112-31....

# Literatuur:


David Kahn, 'The Codebreakers', New York 1967
K. de Leeuw en H. van der Meer, 'A homophonic Substitution in the archives of the last great pensionary of Holland', artikel uit 'Cryptologia', deel 17, nr. 3, juli 1993, Rose Hulman Institute of Technology, Terre Haute, Indiana, U.S.A.
Willem Bilderdijk, 'Speels Vernuft, rebus-brieven en bedriegers', toegelicht door Dr. J. Bosch, 's-Gravenhage 1981
W. Kozaczuk, 'Enigma', Londen 1964
Dan Tyler Moore en Martha Waller, 'Cloak and cipher', 1962
C.L. Levoir, 'Vorstelijk geheimschrift', uit 'Je maintiendrai', Leiden 1905
Gert Holstege, 'Z.O.P.', artikel uit 'Filatelie Informatief', november 1987
Carel Vorstelman, 'Geheimschriften, de avonturen van dr. Malvero, cryptograaf', Amsterdam 1942
Jean-Paul Clebert, 'De zigeuners', 1964
H. van Maanen, 'Colossus, de eerste computer...', artikel uit het Parool, 5 mei 1990
Paul Hoffman, 'De wraak van Archimedes', 1988
Toon Tellegen, 'Toen niemand iets te doen had'.




# Foto's

Algemeen rijks Archief: 17r,21 / Collectie Dortmund: 26 / Koninklijke Bibliotheek: 1,7,8o, 10,13,25l / Koninklijk Huis Archief / 24 / Letterkundig Museum: 22,23 / Philips Usfa: 29 / Het Nederlandse PTT museum: 8b,16b,17g,19r / Rijksarchief voor de Centrale Regeringsarchieven vanaf 1795: 10,11l,15,20 / Rijksmuseum voor Oudheden: 3,4, / Scryption: 16o,25,28m

# Met dank aan:


Drs. J.A.A.M. Biemans, Museum Dortmond, Amsterdam
Mevr. J. de Bie, PTT museum, Den Haag
Dhr. J. Camping, Museum Verbindingsdienst, Ede
Dhr. M. van Hattum, Bilderdijk museum, Amsterdam
Dhr. R. Haubourdin, Algemeen Rijks Archief, afd. Kaarten en Tekeningen
Prof. dr. G. Holstege, voor de verzameling Z.O.P.
Mr. R. Huijbrecht, Rijksarchief in Zuid-Holland
Drs. Th.J.H. Krispijn, faculteit der Assyriologie van de Rijks Universiteit Leiden
Drs. K. de Leeuw, Universiteit van Amsterdam
Mevr. J. van Otterloo, Sectie Militaire Geschiedenis Koninklijke Landmacht
Dhr. S.F.M. Plantinga, Algemeen Rijksarchief
Prof. dr. ir. W.L. van der Poel, faculteit der Technische Wiskunde en Informatica, TU Delft
Dr. M.J. Raven, Rijksmuseum voor Oudheden
Dhr. T. Vermeulen, Koninklijke Bibliotheek
Koninklijk Huis Archief
Letterkundig museum
Rijksarchief voor de Centrale Regeringsarchieven vanaf 1795
Ir. J.A. Kelderman, afd. Informatica, TU Delft
Mevrouw T.J. Hoogenboezem


# Index



# Colofon


Uitgave naar aanleiding van de expositie Geheimschrift – Speuren naar Verborgen Boodschappen, gehouden in het Scryption van 14 december 1993 t/m 16 mei 1994.
Samenstelling en tekst: Agnes Vugts, Carine van Vugt
Vormgeving: Rob Berkel, Marielle Brands
Zetwerk en druk: Meboprint Amsterdam
Dit is nummer:

Scryption

**Techniek en vormgeving van schrift en kantoor**
**Spoorlaan 434a, Tilburg (013) 353777**