

Een roostergeheimchrift van Alexander Baron van Spaen (1775–1811)*

Karl de Leeuw Hans van der Meer†

Summary

After the retreat of the English and Russian troops from Dutch soil in 1799, the Batavian Directory sought means to end its participation in the war against England. It wanted to end hostilities bilaterally, that is to say without negotiations for a general peace. It hoped for mediation from Prussia, that already negotiated a separate peace with France in 1795. The Directory tried to make the idea acceptable to the British — who wanted to see the former Stadtholder of the Dutch Republic back in charge — by asking the Stadtholder’s son, the Hereditary Prince William, to act as new head of state, more or less modelled on the French example of Napoleon’s ‘consulate.’

The former Stadtholder and his family were to be approached by Alexander van Spaen, a young nobleman who was a personal friend, both of the Batavian Director in charge of Foreign Affairs, Hugo van der Goes, and the Hereditary Prince. The diplomatic manoeuvring that accompanied the mission of Alexander van Spaen required the exchange of several letters between the Hereditary Prince and Alexander, most of them during the summer of 1800. The letters were enciphered by means of a remarkable variant of a turning grille, a device described for the first time only five years before in a mathematical magazine. The origin of this particular variant remains unknown, but its application shows a profound understanding of cryptography.

1 Inleiding

Met zijn formidabele boek *The Codebreakers* grondvestte de Amerikaanse journalist David Kahn de geschiedschrijving van de cryptografie en opende tevens nieuwe wegen voor de geschiedschrijving [1]. In dit boek wordt echter relatief

* Wij zijn Hare Majesteit de Koningin erkentelijk voor toestemming om onderzoek te doen in het Koninklijk Huisarchief.

† Published in: *De Achttiende Eeuw*, 25 (1993) 2, 187–210

weinig aandacht besteed aan het gebruik van geheimschrift gedurende de achttiende eeuw. De door hem gegeven voorbeelden hebben grotendeels betrekking op de Amerikaanse Onafhankelijkheidsoorlog en worden gepresenteerd in het veel bredere kader van het gebruik van geheimschrift vóór de uitvinding van de telegraaf [2]. Deze benadering lijkt te zijn ingegeven door het feit dat de wat meer gecompliceerde geheimschriften die in de Renaissance zijn ontstaan, vóór de tweede helft van de negentiende eeuw betrekkelijk weinig werden toegepast.

De hoofdrol was in deze periode weggelegd voor de ‘nomenclatuur’, een meer of minder uitgebreide lijst van namen en begrippen, die gesubstitueerd konden worden door getallen. Het verschil tussen een geheimschrift en een nomenclatuur of code kan als volgt worden gekarakteriseerd. Bij het omzetten van een bericht in geheimschrift wordt een voorschrift in combinatie met een voor het bericht specifieke sleutel gehanteerd. Het voorschrift is doorgaans eenvoudig van aard en de sleutel een gemakkelijk te onthouden letter- of cijfercombinatie. Het resultaat is (meestal) een letter-voor-letter vervanging en/of verwisseling. Het gebruik van een nomenclatuur komt neer op het vervangen van letters, lettergrepen, woorden en uitdrukkingen door codegroepen opgenomen in een lijst, het codeboek.

Deze nomenclaturen vervulden vooral een functie bij de beveiliging van diplomatieke correspondentie. De samenstelling was veelal in handen van ambtenaren die tevens belast waren met het decoderen van onderschepte berichten van vreemde gezantschappen [3]. Kahn gaat echter niet in op het feit dat in de achttiende eeuw een toenemend gebruik van geheimschrift valt te constateren. Dit geldt met name voor het laatste kwart van de eeuw en valt globaal samen met wat door R.R. Palmer ‘the Age of Democratic Revolution’ is genoemd [4].

Aangezien grote politieke en sociale spanningen sommige staten op de rand van een burgeroorlog brachten en hierdoor velen ten prooi vielen aan een collectieve achtervolgingswaan, schreven diplomaten en andere individuen in hun particuliere correspondentie veelvuldig in een geheimschrift. Veel gecodeerde documenten bevinden zich nog in achttiende-eeuwse archiefbestanden. De behoefte aan modellen en voorbeelden van geheimschriften blijkt wel uit de publikaties hierover aan het eind van de achttiende eeuw [5].

In de meeste boekjes lag het accent op monoalfabetische substitutiecijfers en wel op manieren om die te construeren. Daarnaast werden één of meer polyalfabetische systemen behandeld, waarbij varianten van de Vigenère de meeste belangstelling genoten. In het monoalfabetisch substitutiesysteem wordt elke letter door een vaste andere letter vervangen, terwijl in een polyalfabetisch systeem deze vervanging wisselt met de plaats in het bericht. In het Vigenère systeem wordt elke letter vervangen door een die een aantal plaatsen verder in het alfabet staat; dit aantal wisselt volgens een bepaalde sleutel met de positie in de tekst.

De meeste auteurs raden het gebruik van ‘le chiffre indéchiffable’ (d.i. het Vigenère systeem) alleen in uitzonderlijke gevallen aan. Het monoalfabetisch substitutiecijfer werd kennelijk nog betrekkelijk veilig gevonden. Zelden staan in de publikaties over geheimschriften technieken beschreven om een monoalfabeet te breken. Dit is merkwaardig, want die methoden werden al in de

Renaissanceperiode ontwikkeld [6]. Diderot en d'Alembert vormen in dit opzicht een uitzondering. Dit heeft alles te maken met het feit dat Diderot de de cryptografie niet ziet als een statische verzameling technieken, maar als een veranderend vakgebied met een geheel eigen logica [7]. De encyclopedisten onderscheiden zich hiermee van hun tijdgenoten, die de indruk wekken eigen of tenminste nieuwe vindingen te presenteren [8]. Bestudering van deze, of andere, gedrukte bronnen zou gemakkelijk Kahns beeld kunnen bevestigen dat de achttiende eeuw geen originele bijdrage heeft geleverd aan de geschiedenis van de cryptografie. Het is echter niet aan te raden om bij de geschiedschrijving van de cryptografie uitsluitend af te gaan op handboeken. De cryptografische praktijk werd gedomineerd door een kleine groep ambtenaren die betrokken waren bij het coderen en decoderen van berichten. De kennis op dit gebied werd zoveel mogelijk geheim gehouden, maar was niet uitsluitend voorbehouden aan specialisten. Ook de opdrachtgevers, koningen en ambassadeurs, streefden naar eigen kennis op dit gebied om de prestaties van hun 'zwarte kamers' te kunnen beoordelen of onafhankelijk van hun ambtenaren te kunnen opereren [9]. Vermoedelijk ontwikkelden de technieken en methoden van de geheimschriften zich vooral in de politieke machtscentra, maar deze werden om begrijpelijke redenen niet gepubliceerd. In ieder geval lijkt het de moeite waard om te onderzoeken hoe het proces van interactie tussen theorie en praktijk verlopen is en welke factoren daarbij een rol hebben gespeeld.

In dit artikel zal getracht worden dit proces aan de hand van een case-study te reconstrueren. De case-study betreft de zending van Alexander baron van Spaen naar Berlijn in het jaar 1800 door de Bataafse Agent voor de Buitenlandse Betrekkingen, Maarten van der Goes. Deze zending heeft weinig of geen aandacht gekregen in de literatuur over de Bataafse Republiek, maar is op grond van Colenbranders *Gedenkstukken* goed te volgen. Colenbrander besteedt echter geen aandacht aan het aspect dat ons in dit verband het meest interesseert: de gecodeerde correspondentie die zich in het kader van de zending ontwikkelde tussen Van Spaen en de erfprins.

2 Missie van Alexander baron van Spaen

In 1800 trachtte het Bataafse Directoraat een einde te maken aan de betrokkenheid van ons land bij de oorlog tegen Engeland. De verworvenheden van de Bataafse Revolutie werden in eigen land nog steeds gewaardeerd, maar de door de Fransen opgelegde retributies en de hinder die de buitenlandse handel van de oorlog ondervond drukten zwaar op de economie. De gedachten van de Bataafse regering gingen uit naar een door de grote mogendheden gegarandeerde neutraliteit in ons land. Dit zou moeten geschieden na terugtrekking van de Franse bezettingsmacht en legering van Pruisische troepen in enkele vestingsteden en onder handhaving van de bestaande staatsinstelling. De Bataafse autoriteiten gaven er de voorkeur aan dat het initiatief tot de door hen gewenste regeling genomen zou worden door de regering te Berlijn, die weer zou moeten handelen op uitnodiging van Engeland [10].

De stadhouderlijke familie leek, met haar goede contacten aan de Engelse en Pruisische hoven, geschikt om als pleitbezorger op te treden. De Bataafse Agent van Staat voor de Buitenlandse Betrekkingen, Maarten van der Goes, werd belast met de verdere uitwerking. Om de stadhouderlijke familie te benaderen schakelde hij een voormalige infanteriekapitein uit het Staatse leger in, die geen trouw had willen zweren aan de Bataafse Republiek maar die zich evenmin had aangesloten bij het zogenaamde rassemblement van Osnabrück, een Oran-gistische troepenformatie die een poging had willen ondernemen de Bataafse Republiek omver te werpen. Het ging om Alexander baron van Spaen (1775–1811), een persoonlijke vriend van Van der Goes en een zoon van Willem Anne baron van Spaen LaLecq (1750–1818). Van Spaen LaLecq had onder het restauratie regime in de periode 1787–1795 een prominente rol gespeeld en beschikte niet alleen over goede contacten met de Oranjes, maar ook met het Pruisische hof. Alexander was bijzonder geschikt voor deze missie omdat hij de erfprins goed kende uit de tijd dat hij nog diende in het Staatse leger [11].

Alexander van Spaen vertrok in maart 1800 naar Engeland en hij bleef daar tot begin april. De stadhouderlijke familie wist inderdaad een onderhoud voor hem te arrangeren met lord Grenville, de Engelse minister van buitenlandse zaken. Deze wees het initiatief niet direct van de hand, maar stelde drie voorwaarden voor een eventuele Engelse deelname: (1) directe legering van Pruisische troepen die een eventuele terugkeer van de Fransen met geweld zouden kunnen verhinderen; (2) herstel van het stadhouderlijk gezag en (3) een garantie dat de neutraliteit van ons land niet gebruikt zou worden om het Engelse handelsembargo tegen Frankrijk te ontduiken [12]. Lord Grenville verwachtte niet dat de Bataafse autoriteiten aan alle eisen tegemoet zouden kunnen komen, maar in Den Haag hoopte men een compromis te kunnen vinden, waarbij de erfprins de rol van staatshoofd op zich zou kunnen nemen.

Op 16 april van hetzelfde jaar namen de Bataafse autoriteiten het besluit ook het Pruisische hof te benaderen. Alexander van Spaen werd opnieuw ingeschakeld als tussenpersoon, ditmaal mede op aanraden van prinses Wilhelmina, bij wie hij kennelijk in de smaak was gevallen. In Berlijn werd de zaak voorbereid door de erfprins, die op dat moment in die stad verbleef en die getrouwd was met een zuster van de Pruisische koning, alsook door generaal De Stamford, een vertrouweling van de stadhouderlijke familie [13]. Van Spaen werd begin mei ontvangen door de Pruisische premier Von Haugwitz. Deze hield zich in het gesprek op de vlakte, maar voelde er even weinig voor als de Engelse regering. Hij vreesde dat een Pruisisch initiatief in deze richting op korte termijn nadelig zou kunnen zijn voor de relatie met Frankrijk. Bovendien bracht de legering van Pruisische troepen in de Bataafse Republiek het gevaar met zich mee van een militaire confrontatie. Hij stelde, na overleg met de Pruisische koning, voor de Bataafse regering het plan zelf ter sprake te laten brengen in Parijs [14].

Daarmee ontstond een situatie die het Directoraat in eerste instantie had willen vermijden. Het hoopte de stemming in Parijs echter te kunnen beïnvloeden door omkoping van enkele sleutelfiguren in de Franse regering. In eerste instantie werd gesproken over een bedrag van een kleine twee miljoen pond, te verdelen

onder mevrouw Bonaparte, Talleyrand en Sémonville; later werd ook het tienvoudige genoemd. Dit laatste maakte de stadhouderlijke familie achterdochtig, omdat de de Bataafse autoriteiten zo'n grote som onmogelijk konden fourneren zonder medewerking van de Nationale Vergadering. De indruk bestond dat de Bataafse regering verwachtte dat de Engelsen voor het geld zouden zorgen, maar hierover was niets afgesproken [15].

3 Briefwisseling Alexander van Spaen en de erfprins

De reis van baron Van Spaen naar Berlijn was voorbereid door prinses Wilhelmina, die haar zoon, de erfprins, op de hoogte had gebracht van van Spaen's activiteiten en het standpunt der Engelse regering [16]. Er zijn geen aanwijzingen dat de erfprins en Van Spaen over de voorbereiding van diens reis rechtstreeks contact hebben gehad. De briefwisseling lijkt vooral tot doel te hebben gehad de erfprins, die op 20 mei naar Engeland vertrok, te informeren over de resultaten, niet alleen in Berlijn, maar ook in Parijs en Den Haag. De inhoud van de correspondentie, die in totaal 8 brieven omvat, allen geschreven tussen 9 mei en 5 december 1800, kan worden gedestilleerd uit de bijgevoegde transcripties en minuten van de erfprins, die ook door Colenbrander zijn gebruikt voor diens bronnenpublicatie. De twee laatste brieven van Van Spaen, die van 13 juli en 5 december, zijn niet door Colenbrander gesignaleerd, maar konden op basis van het gebruikte geheimschrift door ons met de overige brieven in verband worden gebracht [17].

De briefwisseling tussen Alexander van Spaen en de erfprins begon op 9 mei 1800, een dag na het onderhoud met Von Haugwitz over de wensen en ideeën van de Bataafse regering. Van Spaen geeft een korte samenvatting van het besprokene en verklaart teleurgesteld te zijn over het feit dat von Haugwitz geen duidelijk standpunt had willen innemen. Het is niet meer na te gaan of deze eerste brief al in geheimschrift is gesteld want het origineel is niet meer voorhanden. Wij moeten het doen met een afschrift dat, te oordelen naar het handschrift, gemaakt is door de secretaris van de erfprins. Uit het feit dat er een afschrift is gemaakt zou men kunnen afleiden dat de brief inderdaad in geheimschrift is geschreven, maar zowel schrijver als ontvanger verbleven op dat moment in Berlijn. Het is niet uitgesloten dat de brief is overgebracht door een bode of door Van Spaen zelf is afgegeven [18].

De tweede brief dateert van 3 juni en hiervan is het gecodeerde origineel nog wèl aanwezig. De brief is evenals de vorige geschreven in Berlijn, maar de erfprins was reeds op 31 mei vertrokken naar zijn ouders in Londen, waar hij op 20 juni arriveerde [19]. Van Spaen vat hierin samen wat Van der Goes hem schrijft over de Bataafse pogingen in Parijs om Napoleon om te kopen. De resultaten zijn tot dusver niet bemoedigend, maar de Bataafse Directeuren hopen dat de Oostenrijkse militaire successen in Italië de Fransen tot een grotere inschikkelijkheid bewegen zullen. Van Spaen vraagt de erfprins of hij van mening is dat alle pogingen moeten worden opgegeven als Napoleon niet meteen akkoord

wil gaan met een eventuele neutraliteit van ons land en de Pruisen niet meer van zich laten horen [20].

Op 21 juni volgt de derde brief, ook ditmaal gecodeerd. Van Spaen brengt hierin opnieuw het laatste nieuws over de ontwikkelingen in Parijs, zoals hij dat heeft vernomen van Maarten van der Goes. De Pruisische zaakgelastigde heeft bij de Franse autoriteiten gewezen op de wenselijkheid van neutraliteit. Talleyrand en Joseph Bonaparte hebben zich gereserveerd opgesteld, maar niettemin getracht de eerste consul voor het project te interesseren. De baron stuurt bij deze gelegenheid een pakket mee, waarvan hij de inhoud niet kent maar dat, getuige het handschrift, afkomstig is van mevrouw Van Heeckeren van Enghuizen [21].

Op 6 juli volgt de vierde brief van Van Spaen aan de erfprins, opnieuw in geheimschrift. Van Spaen schrijft hierin dat door de Franse successen in Italië het voor Napoleon niet langer urgent is om een aparte regeling te treffen voor de Bataafse Republiek. Het Franse staatshoofd heeft bovendien verklaard alleen akkoord te kunnen gaan met een dergelijke regeling, als de Bataafse regering in handen komt van mensen die van de Engelsen niets moeten hebben. Dit zou de oude stadhouder dus uitsluiten, maar niet de erfprins als Napoleon van diens ware gevoelens op de hoogte zou worden gebracht [22]. Van Spaen wil weten wat de erfprins hiervan vindt [23].

De vijfde brief van Van Spaen is geschreven op 13 juli en eveneens afkomstig uit Berlijn. Hij meldt hierin dat Von Haugwitz hem heeft laten weten dat de koning naar aanleiding van het rapport van zijn ambassadeur Sandoz Rollin in Parijs besloten heeft geen initiatieven meer te nemen. Van Spaen trekt hieruit de conclusie dat zijn aanwezigheid in Berlijn geen nut meer heeft en kondigt zijn vertrek aan naar Den Haag [24].

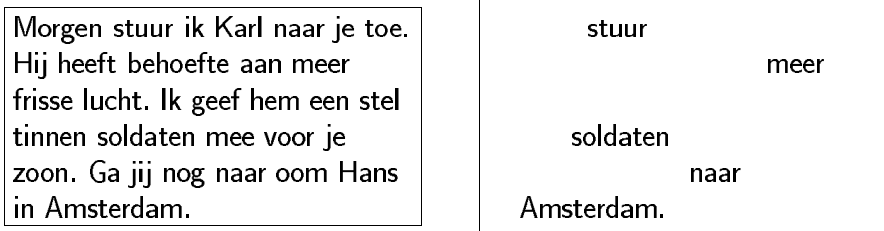
Op 26 juli formuleert de erfprins een antwoord. Hij verblijft op dat moment in Londen en uit de aanhef valt op te maken dat de drie laatste brieven van Van Spaen niet zijn doorgezonden naar het eiland Wight, waar hij de voorafgaande weken had doorgebracht. Uit het handschrift van de klaartekst valt op te maken dat Van Spaens brieven door de erfprins zelf werden opgelost (en dus niet door diens secretaris of prinses Wilhelmina). Van het antwoord is alleen de minuut blijven bestaan, maar het lijkt ons onwaarschijnlijk dat de verzonden versie niet zou zijn gecodeerd. De erfprins meldt over de kwestie met lord Grenville gesproken te hebben. Hij gelooft niet dat de Engelse regering bereid zal zijn mee te werken aan een poging Bonaparte om te kopen. Hij concludeert dat er niet veel meer uit te richten valt. Hij raadt Van Spaen aan, mocht hij het in Berlijn niet willen opgeven, contact op te nemen met de Engelse gezant Cerysfort, die van lord Grenville over deze kwestie enkele instructies heeft meegekregen [25].

De correspondentie tussen Van Spaen en de erfprins is hiermee niet ten einde. Op 10 oktober schrijft de erfprins een tweede brief die helaas verloren is gegaan. Op 5 december volgt weer een brief van Van Spaen. De baron maakt hierin melding van de brief van de Bataafse gezant in Berlijn, Bourdeaux, aan Maarten van der Goes, waarin sprake is van Pruisische plannen om de erfprins in het kader van de komende vredesregeling ergens als staatshoofd te installe-

ren. Ook wordt melding gemaakt van berichten van extraordinaris ambassadeur Schimmelpenninck uit Parijs over een op handen zijnde regeling met Engeland [26].

4 Roostergeheimschriften

In de correspondentie van Alexander van Spaen wordt gebruik gemaakt van een geheimschrift, dat met behulp van een rooster de letters van het bericht verwisselt, een zogenaamde roostertranspositie.

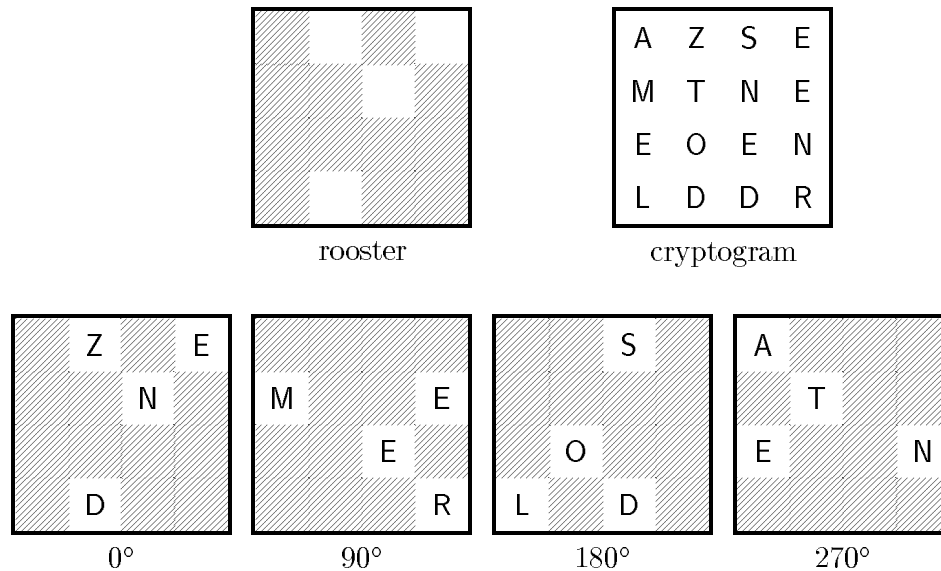


Figuur 1: Rooster volgens Cardano; links verzonden bericht, rechts uitsparingen.

Een roostergeheimschrift vinden we voor het eerst beschreven door de Italiaanse geleerde Cardano (1501–1576) [27]. Het Cardano-rooster of ‘grille’ bestaat uit een stuk perkament, waarin op de schrijfflijn op onregelmatige plaatsen gaten zijn uitgespaard. Men legt dit rooster bovenop een stuk papier en schrijft de geheime boodschap in de uitsparingen (opgesplitst in letters, lettergrepen of woorden, al naar men wenst). Vervolgens wordt het rooster weggenomen en de ruimten tussen de delen van het bericht worden opgevuld. Dit opvullen geschiedt zó, dat het geheel een onschuldige boodschap oogt. Cardano schreef driemaal kopieën van de tekst voor ‘om onregelmatigheden in het handschrift te voorkomen, onregelmatigheden die de boodschap kunnen verraden.’

Een latere vorm van het rooster is de Fleissner-grille, genoemd naar de Oostenrijkse cryptoloog Eduard Fleissner von Wostrowitz [28]. Het verschil met de eerdere vorm is dat het bericht in horizontale en/of verticale richting kan worden aangevuld met loze kolommen en/of rijen. We praten dan vooral over militaire cryptografie. In de militaire communicatie spelen andere factoren een rol dan in de diplomatieke correspondentie. Vooral de opkomst van de telegraaf en de draadloze telegrafie hebben de ontwikkelingen op dit terrein enorm beïnvloed. Onze landgenoot Auguste Kerckhoffs schreef al aan het eind van de vorige eeuw een toonaangevende verhandeling over de eisen die het militaire bedrijf aan de cryptografie stelt [29].

Waarom is de in de achttiende eeuw zo wijd en zijd verbreide nomenclatuur niet aantrekkelijk als communicatiemiddel in militaire operaties? De veelal aanzienlijke omvang van het codeboek in de nomenclatuur heeft tot gevolg dat coderen en decoderen met veel bladeren en zoek gepaard gaat. Dit maakt het



Figuur 2: Turning-grille met „zend meer soldaten” → AZSEM TNEEO ENLDD R.

werken met een code tijdrovend in vergelijking met het gebruik van een eenvoudig geheimschrift, zoals het roostergeheimschrift. Het geheimschrift vraagt slechts het onthouden van een simpel voorschrift en een betrekkelijk korte sleutel; de benodigde hulpmiddelen zijn klein en gemakkelijk te dragen. Door wisseling van de sleutel kan men snel het geheimschrift variëren, waar deze operatie bij een nomenclatuur de productie van een geheel nieuw codeboek verlangt. Het is daarom niet verwonderlijk dat het gebruik van nomenclaturen in het militaire bedrijf minder ingang heeft gevonden dan in het diplomatiek verkeer.

Het roostergeheimschrift voldoet uitstekend aan de eis dat het eenvoudig te hanteren moet zijn en toch een sterk geheimschrift vormen. Het idee van de turning-grille, het draaiend rooster, is gebaseerd op het benutten van alle posities door combinatie van verschillende standen van het rooster. Dit kan onder meer door het rooster vierkant te nemen en de uitsparingen zó te kiezen dat na viermaal een kwartslag draaien alle vakjes eenmaal aan de beurt geweest zijn. Per stand van het rooster komt een kwart van de posities aan de beurt. Het aantal uitsparingen moet precies een kwart van het totaal aantal vakjes zijn [30]. In elk van de opeenvolgende uitsparingen schrijft men een stukje van de boodschap. In figuur 2 wordt als voorbeeld een 4×4 turning-grille gegeven. Deze roosters zijn zelfs in de Eerste Wereldoorlog (van eind 1916–begin 1917) nog korte tijd aan Duitse zijde in gebruik geweest; de verschillende roosters werden aangeduid met codenamen als ANNA, BERTA, CLARA, ... [31]. Zelfs Jules Verne brengt ons in zijn roman *Mathias Sandorf* een bericht gecijferd met een 6×6 turning-grille en laat ons meegenieten van de ontcijfering [32].

Minder bekend is dat het genoemde boek van Fleissner von Wostrowitz niet de vroegste plaats is, waar dit soort rooster wordt beschreven. De oudste

verwijzing die deze auteurs hebben kunnen vinden is van C.F. Hindenburg in een artikel uit 1796 ‘Fragen eines Ungenannten über die Art durch Gitter geheim zu schreiben’ [33]. Dit artikel wekt sterk de indruk te zijn geschreven op instigatie van iemand die onbekend wil blijven, maar aan Hindenburg wel bekend is. Het beschreven geheimschrift is zonneklaar een turning-grille. Hindenburg laat zien hoe een rooster kan worden geconstrueerd en berekent het aantal mogelijke roosters. De gehele beschrijving maakt de indruk van een in gebruik zijnd systeem. Hoewel pure speculatie, is het verleidelijk om te veronderstellen dat de inspiratie voor het artikel uit militaire kring komt.

Heel aardig is de wijze waarop Hindenburg elk mogelijk rooster van een volgnummer voorziet en dan aangeeft hoe datzelfde volgnummer weer kan dienen voor de constructie van het bijbehorend rooster. Het werkt ongeveer als volgt [34]. Verdeel het rooster overlans en overdwars in tweeën, waardoor vier kwadranten ontstaan. Elke positie in het rooster kan nu door draaien rond het middelpunt worden overgevoerd in een plaats binnen het eerste kwadrant. We kunnen omgekeerd ook zeggen: neem een positie in het eerste kwadrant en kies vervolgens welke van de vier overeenkomstige posities (na resp. 0, 1, 2 of 3 stappen draaien) voor de uitsparing in het rooster in aanmerking komt.

Als voorbeeld werken we het rooster van figuur 2 uit. Dit is een 4×4 rooster en een kwadrant telt $2 \times 2 = 4$ vakjes. Het zal d.m.v. een getal van vier cijfers worden gekarakteriseerd: één cijfer voor de draaiing van elk vakje uit het kwadrant linksboven.

We beginnen met het vakje in de linkerbovenhoek (in het cryptogram rechts in die figuur staat op deze plaats een A). Als we een kwartslag rechtsom draaien komt dit vakje terecht op de plaats van het vakje in de rechterbovenhoek. Omdat één kwartslag draaien genoeg is om het gekozen vakje op een open plaats te brengen noteren we hiervoor het cijfer 1. Nu nemen we het tweede vakje op de bovenste rij (Z in het cryptogram rechts). Dit vakje is al open — d.w.z. nul keer draaien — hetgeen we aangeven door het neerschrijven van een 0. Dan richten we ons op het eerste vakje van de tweede rij (M in het cryptogram rechts). We zien dat driemaal een kwartslag draaien nodig is voordat dit vakje op een open plaats belandt (het open vakje op de onderste rij). Daarom schrijven we een 3 op. Tenslotte nemen we het vierde en laatste vakje van het eerste kwadrant (T in het cryptogram rechts) en zien dat dit na één kwartslag op een open plaats komt; we schrijven dus weer een 1.

Achter elkaar geschreven leggen de gevonden cijfers het gatenpatroon van het rooster eenduidig vast. Voor het rooster van figuur 2 is dat dus 1031. Andersom redenerend kan uit de cijfercombinatie eenduidig worden geconcludeerd tot het gatenpatroon van het rooster. Eigenlijk gebeurt niets anders dan dat de roosters in het 4-talig stelsel worden geteld.

5 Analyse cryptogram van Alexander van Spaen

De eerste reproductie toont (fig. 3) blad I van de drie bladen van de brief van Alexander van Spaen gedateerd Berlijn 13 juli 1800, de tweede reproductie (fig. 4)

de in het archief gevonden gedecodeerde versie van de brief. De transcriptie van de gehele gecodeerde brief is in tabelvorm opgenomen. We zullen laten zien hoe uit de gecodeerde en gedecodeerde tekst de vorm van het gebruikte rooster kan worden afgeleid.

Dit cryptogram vormt op alle drie bladen een rechthoek van 12 rijen en 16 kolommen. De cryptografische eenheid is meestal een enkele letter, soms twee of meer (dit laatste komt vooral voor op blad III). De punten, die achter een deel van de letters staan, hebben we in de transcriptie meegenomen. Ze vallen op, zowel door hun grote aantal als door de letters waar ze achter staan: a, e, n, r, s en t. Tien tegen een dat deze punten het einde van een woord aangeven. Het was immers wel vaker gebruikelijk om de woordstructuur in het cryptogram zichtbaar te maken, teneinde het decoderen ervan te vergemakkelijken. Mogelijk staat er in de transcriptie hier en daar eentje te veel; dat komt dan door de kwaliteit van de fotokopie vanwaar de transcriptie gemaakt is. Eveneens is het niet altijd even gemakkelijk om in het handschrift de ‘c’, de ‘e’ en de ‘l’ van elkaar te onderscheiden. Op enkele plaatsen in het geheimschrift is de daar al neergeschreven letter weer doorgehaald.

Het ligt voor de hand om de drie bladen op te vatten als een in drie delen opgesplitste tekst, waarbij elk deel aan dezelfde crypto-transformatie onderworpen is. Is dit vermoeden juist, dan beschikken we over drie parallelle vertalingen, hetgeen de reconstructie van het rooster immens vereenvoudigt, zoals in het vervolg zal blijken. In combinatie met de klare tekst verwachten we systeem en sleutel zonder al te veel moeite te kunnen reconstrueren. De letters van het cryptogram vertonen zo op het oog een verdeling die goed overeenkomt met de in het Frans gestelde klare tekst. In feite was het op grond daarvan, dat we al snel het vermoeden kregen hier met een roostertranspositie te maken te hebben.

Het systeem kan geen turning-grille zijn, want het is niet vierkant: er zijn 12 rijen van elk 16 cryptografische eenheden. Na het bepalen van de oplossing zullen we zien dat het wel een ingenieuze variant daarop is. Bepaling van de volgorde van de drie delen van de brief is eenvoudig. Het eerste deel maakt zich als zodanig kenbaar door de dagtekening ‘Berlin le 13 de Juillet 1800.’ Het derde deel verraadt zijn aard door de vele er in voorkomende meerletterige tekstfragmenten. Kennelijk wilde de schrijver geen vierde deel beginnen en perste het slot van de brief daarom samen.

We zullen uitgaan van de veronderstelling dat de drie delen aan dezelfde transpositie onderworpen geweest zijn, zodat we de drie delen steeds naast elkaar kunnen leggen. Een begin vinden we al snel rechtsonderaan in deel III met de opvallende groepen ‘Be’, ‘rl’ en ‘in’ op posities III.12.11, III.12.13 en III.12.16. We kijken meteen naar de overeenkomstige posities in de beide andere delen:

	12.11	12.13	12.16
I.	e	n	t.
II.	e	s.	r
III.	Be	rl	in

Berlin ce 10 de Juillet 1800.

e é m a m r e m o d f e e a p m
 l n g s r o e e l i e y a n r e
 s r e u t u p r o x e i n m s r
 e a s e m f s a c r i l o a p a
 c r r i o e a n b t n s l e n s
 u s a e d n i d s e e e s e B s
 a o u c n m o s n o t m a n e u
 p t d n a q e i r q r u o u t e
 t e t e r r r e u a m q l'oe o u
 p e t H f v e a s u a e l y r i
 e s s e i t e g t u z i s e o d n
 u f e e i k i e a o e n n m n t

Figuur 3: Blad I van brief Alexander van Spaen.

Paris le 13 de Juillet 1800.
 Monseigneur S. M. Crainin, ou ce sont
 que trop vérifiées malgré le rapport
 favorable de Bonaparte que j'ai eu
 l'honneur de porter à le Commissaire
 ce de V. A. Altep & que de même si
 me vis surpris de communiquer
 à Mr de Hauquints, ses Excellence
 m'a dit que sa Majesté s'estoit décidé
 d'après les rapports de Mr. Audoz Rollis
 à ne faire aucune démarche ultérieure
 et rompre la négociation. J'ai de vifs
 regrets de l'absence de V. A. Selon
 vils misérablement bien précieux. L'im-
 tité de nos jours bonnavant à Berlin
 m'a décidé à me rendre à la Haye si
 prendrai la liberté de continuer
 d'informer V. A. de quelques nouvelles
 faits que les circonstances peuvent
 arriver & j'ai l'honneur d'être
 de
 A. de Spaen
 1800

Figuur 4: Klare tekst van brief Alexander van Spaen.

Brief 13 juli 1800 van A. de Spaen																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.	e	e	m	u	m	r.	e.	m	o	d	j	e.	e.	a	p	m
2.	l	n	g	s	r	o	e.	e	l	i	e	g	a.	n	r	e
3.	s	r	e	u	t	u	p	r.	o	×	e	i	n	m	s.	r.
4.	e	a.	se.	e	m	f	s.	a	c	v	r	l	o	a	p	a.
5.	c	r	r	i	o	e	a	n	b	t	n	s	l	e	n	s
6.	e.	s.	a	e.	d	n	i	d	s	e.	e.	e.	s	c	B	s
7.	a	o	u	e.	n	m	o	s	n	o	c	m	a	n	e.	u
8.	p	t.	d	n	a	q	e.	i	v	q	r	u	o	u	t	e.
9.	t	e.	t	e	r	r	r.	e.	a.	a	Mr.	q	l	de.	o	u
10.	p.	e.	t	H	j	v	e	a	s	u	a	e	s	g	r	i.
11.	e.	w	e	i	t.	e	q	t	u	z.	i	s	e.	o	d	n.
12.	u	f	E	l'	i	h	e	e	x	o	e	n	n	m	n	t.
deel I																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.	e	d	c	t.	e.	a.	l'	a	e	r	a	o	b	p	m	s
2.	p	l	o	l	r	p	t	e	s.	n	e	c	d	e.	e.	m
3.	n	r	Mr	a.	e.	e	s	d	a	i	l	e.	n	t.	d	a.
4.	e.	n	d	q	v	o	u	z.	e.	a.	s	e	n	a.	o	g
5.	o	t	e	m	c	r	f	a	a	j	i	e.	i	e	a	a
6.	r	s	t	l	e.	t	i	t	o	e	a	e.	n.	s	u	s
7.	J	s	c	e	a	e.	u	t	n	a	i.	×	e.	i	d	s
8.	d	i	e.	e	e	t.	v	s.	i	c	m	d	f	o	a	e
9.	c	r	s.	n	i	r	s	e	e	g	i	c	r	l	d	h
10.	e.	e.	e	s.	u	d'	t	m	s.	a	l	a	d	a	p	t
11.	e.	s	l	e	a	e	b	rai	s	t	r	×	e	×	n	×
12.	r	e	bi	i	s.	e	l	c	en.	u	e	r	s.	e.	e.	r
deel II																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1.	i	ta	b	n	nc	u	es.	m	i	e	pe	r.	uv	a.	d	ent.
2.	d	e	e	n.	c	i	i	p	d	r	a	e	e.	c	a.	i
3.	m	n	m	e	f	e	e	u	r	x.	o	n	e	×	er.	r
4.	J'ai.	m	n	L'	l'h	d	i	re	n	a	u	e	L	t	on	r.
5.	v	neur.	a	i	o	d'e	H	l	a	i	t	tre.	y	t	r	avec.
6.	e.	e.	e.	res	j	d	a	pect.	l	mo	e.	e.	t	ns	p	m
7.	e	ei	r	o	s	gn	e	n.	n	s	s	eur.	d	e	e.	de
8.	r	j	d	vo	e	o	e	tre	s.	al	r.	u	e	tes	l	r.
9.	d'	a.	v	se.	o	en	se	em	re	en	nis	l	ts.	si	r	i
10.	e	b	in	me.	e	n	te	Le	rr	tres	r	a	es	hum	v	t
11.	sa	ble	nts.	et	qu	e.	e.	tres	les.	obeis	a	servi	ci	teur.	r	a:de
12.	d	n	Sp	e	t.	c	a.	co	aen.	o	Be	n	rl	ns	t	in
deel III																

Figuur 5: Complete tekst van de gecodeerde brief.

De veronderstelling dat de punten woordscheiders zijn wint aan kracht: ‘ent’ en ‘es’ zijn plausibele wordeinden.

Ook de ondertekening met ‘A. de Spaen’ is gemakkelijk te vinden. Deze begint aan het slot van rij III.11:

	11.16	12.3	12.9
I.	n.	E	x
II.	×	bi	en.
III.	a:de	Sp	<u>aen</u>

Met ‘Ex’ hebben we ongetwijfeld ‘Excellence’ gelokaliseerd, terwijl in deel II het woordje ‘bien’ gevormd wordt. Omdat we ‘Excellence’ in de klare tekst van figuur 4 op ongeveer een derde van boven zien staan (en ‘a:de Spaen’ overduidelijk het slot van het bericht is) moeten we het vervolg van ‘Excellence’ op het tweede blad zoeken:

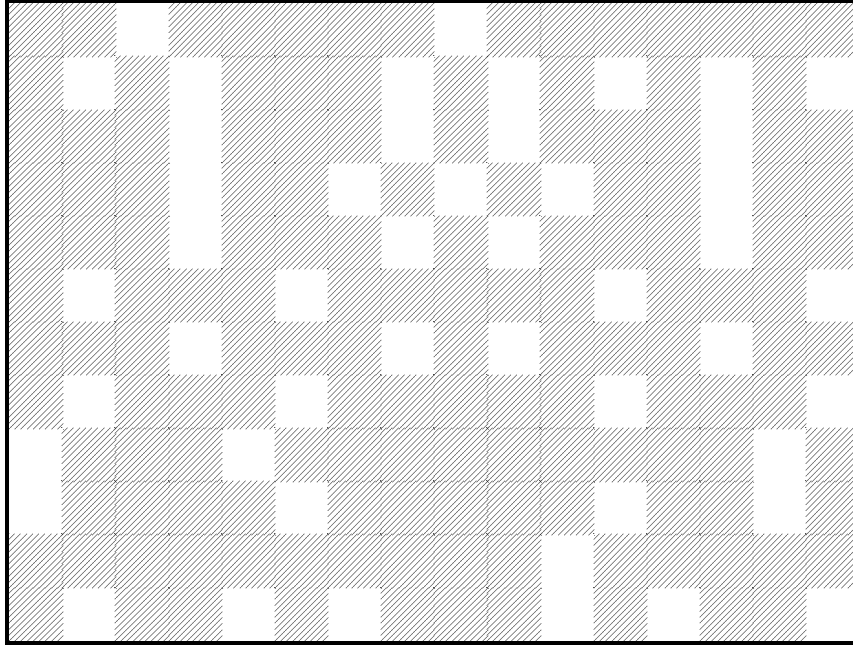
	12.3	12.9	1.3	1.7/9	2.2	2.4	2.8	2.10	2.12	2.14/15
I.	E	x								
II.			c	e	l	l	e	n	c	e.
III.										

De ‘e’ van II.1.5 vertoont een punt en komt daarom niet in aanmerking voor een plaats midden in het woord. Of 1.7 dan wel 1.9, en evenzo 2.14 dan wel 2.15 gekozen moeten worden, kan worden beslist aan de hand van de tekst in de andere delen.

	12.3	12.9	1.3	1.7/9	2.2	2.4	2.8	2.10	2.12	2.14/15
I.			m	e./o	n	s	e	i	g	n/r
I-II.	E	x	c	e	l	l	e	n	c	e.
II-III.	bi	en.	b	es./i	e	n.	p	r	e	c/a
-III.	Sp	<u>aen</u>								

In deel I komt het woord ‘monseigneur’ op. De goede keuze is dus 1.9 en 2.14. In deel III zien we nu ‘bien précieux’ verschijnen [35]. Op deze weg voortgaande komt geleidelijk aan de gehele transpositie aan het licht. Na completering daarvan kunnen we het rooster in z’n geheel reconstrueren en kijken hoe het gebruikt werd [36].

Het blijkt dat we hier niet te maken hebben met een echte turning-grille, maar met een systeem dat er wel veel op lijkt. De functie van het ronddraaien bij de vierkante turning-grille, wordt hier vervuld door het omdraaien van het rooster: voorkant en achterkant verwisselen van rol in de ene draaiing, links en rechts worden verwisseld in de andere draaiing (dus omkeren van het rooster om respectievelijk een horizontale en een verticale as). Voor de volledigheid presenteren we het gehele gereconstrueerde rooster en het ontcijferd cryptogram. Het rooster staat weergegeven in de stand corresponderend met het begin van het bericht.



Figuur 6: Rooster van het cryptogram.

6 Slotbeschouwing

Het gebruik van dit rooster bood Alexander van Spaen en de erfprins grote voordelen. Het was veel veiliger dan de gangbare monoalfabetische substitutie geheimschriften, maar niet zo heel veel moeilijker te hanteren en de kans op fouten was gering. Dit in tegenstelling tot de polyalfabetische systemen als de Vigenère die gemakkelijk fouten opleverde, en tot de nomenclaturen die in het gebruik veel tijd vergden. Het is ook onwaarschijnlijk dat Van Spaen de hier gebezigde techniek zou hebben gekozen zonder op de hoogte te zijn geweest van de discussies op dit gebied, al hoeft dit niet te betekenen dat hij of de erfprins Hindenburgs artikel gelezen heeft. Het ligt meer voor de hand aan te nemen dat het gebruik van deze roosters in bepaalde kringen min of meer courant was en dat Van Spaen en de erfprins een oplossing kozen die hen reeds tot op zekere hoogte vertrouwd was.

De veronderstelling dringt zich op, dat het rooster op de een of andere manier uit de militaire hoek komt. Het is echter onwaarschijnlijk dat dit het Staatse leger is, zoals men wellicht zou kunnen denken omdat beide mannen uit dit leger voortkwamen. De Nederlandse militaire handboeken uit die tijd besteden in het geheel geen aandacht aan dit terrein, terwijl de opleiding en het intellectuele peil van officieren, voorzover zie niet dienen bij artillerie of genie, nog zeer te wensen overliet [37].

Het is ook denkbaar dat Van Spaen het rooster voor dit doel heeft gekregen van iemand anders, bijvoorbeeld van zijn opdrachtgever Maarten van der Goes in Den Haag of van prinses Wilhelmina in Londen. In het eerste geval zou het

monseigneur · × mes · craintes · ne · se · sont · que · trop · verifieent ·
malgre · la · reponse · favorable · de · Buonaparte · que · j'ai · eu · l'honneur ·
de · porter · a · la · connaissance · de · votre · altesse · et · que · de · meme ·
je · me · suis · empresse · de · communiquer · a · Mr · de · Haugwitz · son ·
Excellence · ma · dit · que · sa · majeste · s'etait · decide · d'apres · les ·
rapports · de · Mr · Sandoz · a · ne · faire · aucune · demarche · ulterieure · et ·
a · rompre · la · negociation · J'ai · de · vifs · regrets · de · l'absence · de ·
l'absence · de · votre · altesse · × ses · conseils · ma · serait · bien · bien ·
precieux · × L'inutilite · de · mon · sejour · d'orenavant · a · Berlin · m'a ·
decide · a · me · rendre · a · La · Haye · je · prendrer · la · liberte · de · continuer ·
d'informer · votre · altesse · des · evenements · interessants · que · les ·
circonstances · peuvent · amener · J'ai · l'honneur · de'etre · avec · respect ·
monseigneur · de · votre · altesse · serenissime · Le · tres · humble · et · tres · obeis ·
serviteur · a · de · Spaen

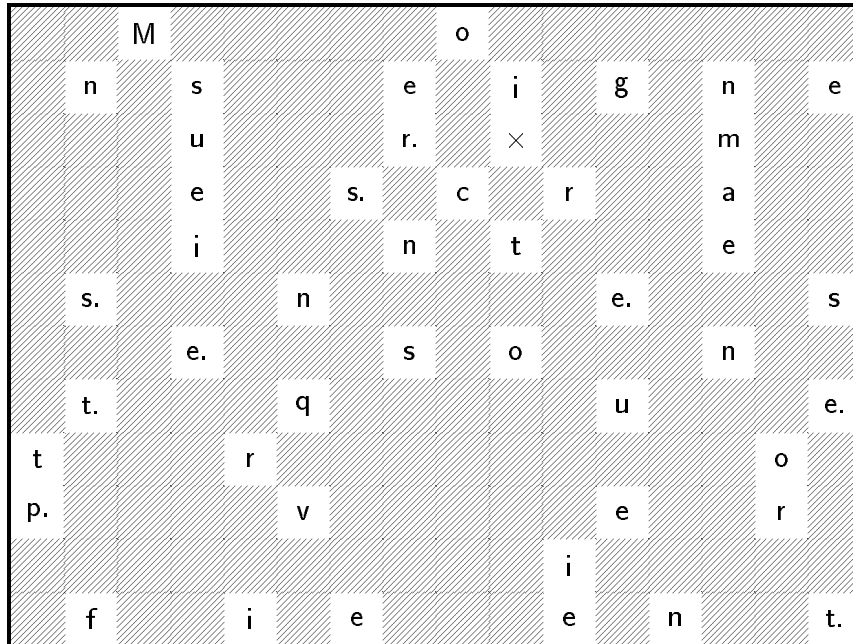
Figuur 7: Ontcijferd cryptogram.

rooster ook gebruikt kunnen zijn in de communicatie tussen Van der Goes en Van Spaen. Dit is niet met zekerheid te zeggen omdat de brieven van Van Spaen aan zijn opdrachtgever verloren zijn gegaan. Het is echter niet zo waarschijnlijk dat Van der Goes veel ervaring met cryptografische technieken had. Bij een eerdere geheime zending naar Berlijn, die van De Vos van Steenwijk in 1799 (met een vergelijkbaar doel), liet hij de keus van een code over aan zijn contactpersoon [38].

De tweede mogelijkheid, prinses Wilhelmina, ligt meer voor de hand. De prinses had al tijdens haar verblijf in Nijmegen in 1787 alle gecodeerde correspondentie van de stadhouder voor haar rekening genomen en dit was, na de restauratie van het stadhouderlijk gezag, zo gebleven voorzover van de diensten van daartoe aangewezen ambtenaren van de Staten geen gebruik kon worden gemaakt [39]. Op Hampton Court lag het hoogtepunt van haar cryptografische activiteit, waarbij het accent lag op de berichtenstroom van en naar Duitsland. Uit de door haar gebruikte sleutels valt op te maken dat zij een goed geheimschrift van een slecht wist te onderscheiden, maar niet dat zij belangstelling had voor transpositiecijfers [40].

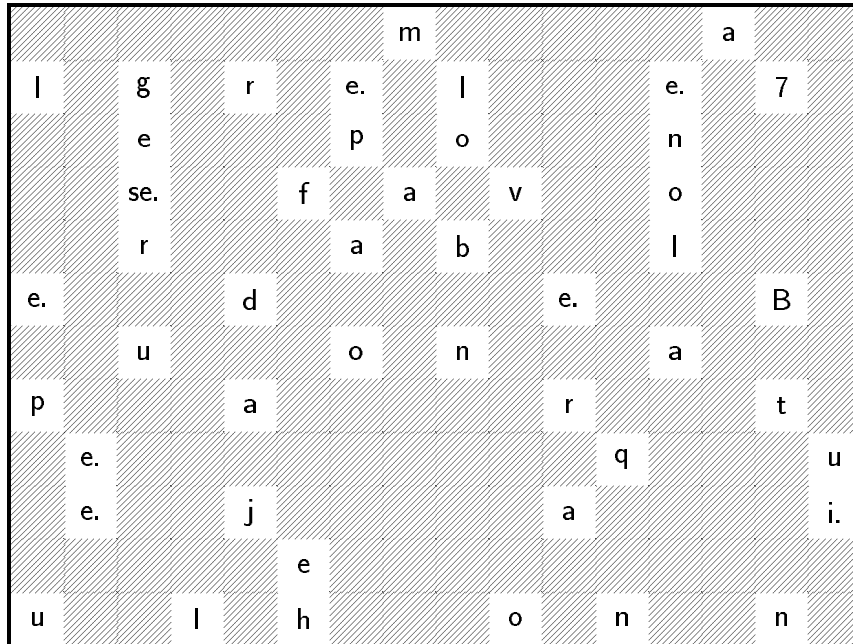
Het lijkt ons het meest waarschijnlijk dat de oorsprong van het rooster gezocht moet worden in de omgeving van de erfprins in Duitsland, bijvoorbeeld aan het Pruisische hof of bij de Pruisische legertop. In dit verband kan uitdrukkelijk worden gedacht aan generaal De Stamford, de man die vanaf 1787 op verzoek van prinses Wilhelmina de militaire vorming van de erfprins voor zijn rekening had genomen. De Stamford had goede contacten met het Pruisische hof en de Pruisische legertop en genoot een zekere reputatie als auteur op het gebied van militaire wetenschappen [41]. Bovendien was hij rechtstreeks bij de missie van Alexander van Spaen betrokken [13].

Het laatste woord over de identiteit van degene die het rooster heeft



Figuur 8: Rooster in positie 1, deel I van het cryptogram.

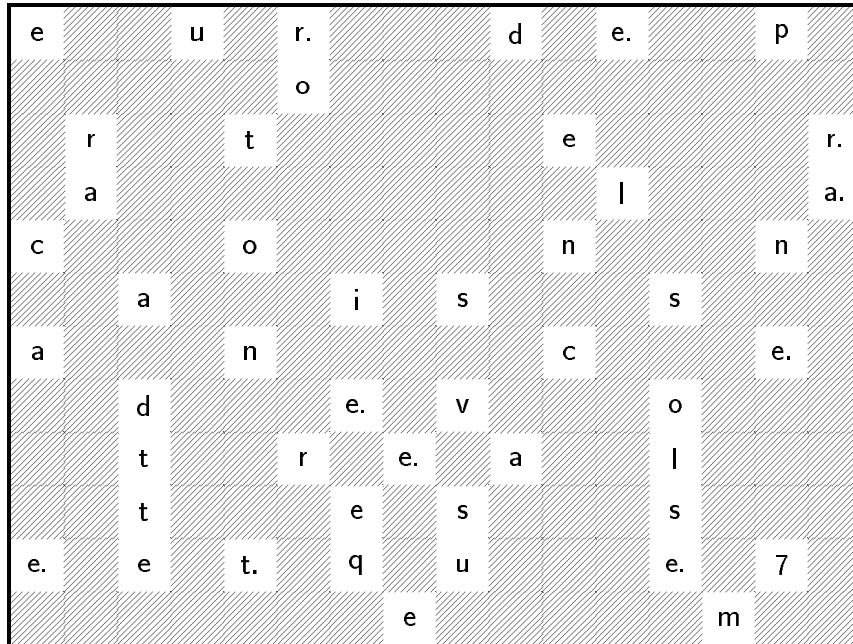
ontworpen is hiermee natuurlijk niet gezegd. Het staat echter vast dat het om iemand gegaan is die grote kennis van zaken had en die beschikte over enige originaliteit, want het gebruikte rooster is niet direct afgeleid van een ons bekend voorbeeld uit de literatuur. Dit onderstreept dat het gebruik van geheimschriften in de achttiende eeuw tot op zekere hoogte los stond van de uit die tijd bekende literatuur. In hoeverre dit geleid heeft tot belangrijke vernieuwingen zal uit vervolgonderzoek moeten blijken.



Figuur 9: Rooster in positie 2, deel I van het cryptogram.

Referenties

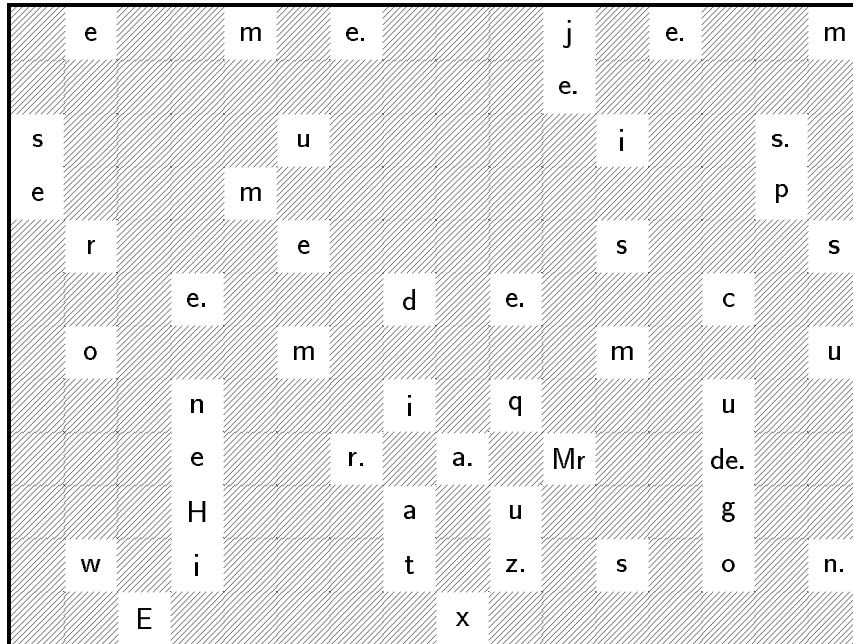
- [1] D. Kahn: *The Codebreakers* (New York, 1967).
- [2] *Ibid.*, p.174–188.
- [3] D. Kahn: *The Codebreakers* (New York, 1967), p.125–174.
- [4] R.R. Palmer: *The Age of Democratic Revolution*(2 dln.) (Princeton 1959 en 1964).
- [5] Diderot: *Encyclopédie ou Dictionnaire Raisonné des Sciences, Arts et Métiers* (1753–1765) deel III p.334, deel IV p.523, p.666–668.
Nederlandstalige voorbeelden zijn: *Werkwijze om te schrijven in dier voege, dat het zonder den sleutel met geene mogelijkheid te ontcijferen is; De geheime Schrijfkunst of briefwisseling: Door een geoefend liefhebber* (Rotterdam, 1794). In de *Geheime Brievenschrijver aangetoond met verscheydene voorbeelden* (Amsterdam, ca. 1760) komt een opdracht voor aan ‘alle legercommandanten, officieren, militairen, etc.’ Dit wijst er op dat ook in de republiek militair gebruik van geheimschrift geen onbekend verschijnsel was.
- [6] D. Kahn: *The Codebreakers* (New York, 1967), p.108–114.
- [7] In dit verband noemt hij het standaardwerk van Gustavus Selenus (pseudoniem voor August Braunschweig-Lüneburg) *Systema integrum cryptographiae* (Lüneburg, 1624). Dit werk genoot in de 18e eeuwse republiek een zekere populariteit. Raadpensionaris L.P. van de Spiegel beschikte bijvoorbeeld over een exemplaar (zie hiervoor de veilingcatalogus met betrekking



Figuur 10: Rooster in positie 3, deel I van het cryptogram.

tot zijn bibliotheek (Utrecht, 1801) 2 dln.), maar ook R.M. van Goens kende dit boek (KB, inv. R.M. van Goens 130D8/D4).

- [8] Dit wordt met zoveel woorden gesteld in J.C.F. Scherber: *Den Dechiffrier. Schlüssel oder Entzifferung deutscher unter unbekannter Characteren versteckter Schrift* (Zelle, 1798).
- [9] Wij ontlene deze stellige indruk aan een inventarisatie van cryptografisch materiaal in het K.H.A. en in het archief van de raadpensionaris Van de Spiegel. Een artikel hierover is in voorbereiding.
- [10] H.T. Colenbrander (ed.): *Gedenkstukken der Algemeene Geschiedenis van Nederland van 1789 tot 1840* ('s Gravenhage, 1905–1922) deel m.b.t. 1798–1801(2), p.1106.
- [11] *Ibid.* p.1100–1101; voor gegevens m.b.t. de familie Van Spaen-LaLecq zie inventaris en archief van de familie Van Spaen bij de Hoge Raad van Adel. Voor gegevens m.b.t. de relatie tussen de erfprins en Alexander, zie *ibid.*, inv.nr. 280, minuut van 27 maart 1798 van W.A. van Spaen LaLecq aan Von Haugwitz; voor Alexanders militaire loopbaan zie: *ibid.*, inv.nr. 494 en ARA, 1e afdeling, Raad van State, inv.nr. 1941 I en inv.nr. 1943 II. Hij was kapitein in het infanterieregiment nr. 5 van Des Villattes (met dank aan de heer H.L. Zwitter).
- [12] *Colenbrander*, p.1106–1109.
- [13] *Ibid.* p.1110–1111.
- [14] *Ibid.* p.314–318; p.612; p.1111–1112.
- [15] *Ibid.* p.1112–1114; p.1116–1119.



Figuur 11: Rooster in positie 4, deel I van het cryptogram.

- [16] *Ibid.* stuknrs 825 en 827 (brieven van 4 en 8 april 1800 van de prinses aan de erfprins) p.1106 en p.1108.
- [17] *Ibid.* p.1120 noot.
- [18] K.H.A., archief koning Willem I, VIIIc S 68, brief van Van Spaen aan de erfprins van 9 mei 1800.
- [19] Colenbrander, p.1114, noot 2.
- [20] *Ibid.*, p.1118.
- [21] K.H.A., archief koning Willem I, VIIIc S 68, brief van 21 juni 1800.
- [22] De erfprins was kritisch gestemd tegenover de Engelsen als gevolg van de ontbinding van het rassemblement van Osnabrück en de bezetting van de Nederlandse koloniën.
- [23] K.H.A., archief koning Willem I, VIIIc S 68, brief van 6 juli 1800.
- [24] K.H.A., archief stadhouder Willem V, inv.nr. 331(7). Deze brief is niet eerder aan Van Spaen toegeschreven, misschien vanwege het onduidelijke onderschrift in de bijbehorende klaartekst. Het gebruikte geheimschrift laat echter geen twijfel bestaan over de afzender.
- [25] Zie noot [21]; minuut van 26 juli 1800.
- [26] K.H.A., archief koning Willem I, VIIIc H 22. Deze brief is anoniem en niet eerder aan Van Spaen toegeschreven. Uit de plaats in het archief en een begeleidend schrijven valt op te maken dat de brief is verzonden via Van Heeckeren van Enghuizen die, als Gelders edelman, wel vaker een rol speelde in de communicatie met de erfprins, als deze in Duitsland verbleef.
- [27] D. Kahn: *The Codebreakers* (New York, 1967), p.144–145.

- [28] E.B. Fleissner von Wostrowitz: *Handbuch der Kryptographie* (Wenen, 1881).
- [29] Auguste Kerckhoffs: *La Cryptographie Militaire* (Paris, 1883), hoofdstuk II, Desiderata de la Cryptographie Militaire, p. 8–10.
- [30] Strikt genomen geldt dit alleen voor een rooster met een even aantal vakjes. Is het aantal oneven dan laat men het middelste vakje buiten beschouwing.
- [31] D. Kahn: *The Codebreakers* (New York, 1967), p.308–309.
- [32] Jules Verne: *Mathias Sandorf* (Paris, 1885); samen met nog twee andere geheimschriften uit resp. *La Jaganda* en *Voyage au Centre de la Terre* te vinden bij A. Lange et E.A. Soudart: *Traité de Cryptographie* (Paris, 1935), p.72, p.311-322.
- [33] C.F. Hindenburg: *Archiv der reinen und angewandten Mathematik*, III p.347–351, V p.81–99, 1796.
- [34] Terwille van de eenvoud is de beschrijving een tikje aangepast.
- [35] Het tweemaal achtereen voorkomen van het woord ‘bien’ vinden we in de klare tekst niet terug. Waarschijnlijk een vergissing van de schrijver van het cryptogram, waardoor men zich niet van de wijs moet laten brengen. Het is nog een keer gebeurd.
- [36] Kleine foutjes in de oplossing — vaak het gevolg van verkeerde interpretatie van de geschreven tekst — komen vanzelf aan het licht bij het ineenpassen van de roostertransformaties en kunnen dan worden gecorrigeerd. Ook bij deze analyse gebeurde dit.
- [37] Voor de vorming van officieren zie: H.L. Zwitser: *De militie van den Staat* (Amsterdam, 1991), p.123. De door ons geraadpleegde militaire handboeken zijn: *Magazijn voor Militaire Wetenschappen* (Arnhem, 1793); J. Dibbetz: *Groot Militair Woordenboek* (’s Gravenhage, 1740); G. van Scharnhorst: *Militair Zakboek* (’s Gravenhage, 1800).
- [38] Deze had een voorkeur voor de *Dictionnaire portatif, en Hollandais et Français* van Pieter Marin en daarvan het tweede deel in de door Ernst Zeydelaar verbeterde negende editie uit 1787, aangevuld met enkele codena-men voor relevante personen en politieke entiteiten. De betreffende woorden werden gewoon aangegeven door het nummer van de pagina in combinatie met het nummer van de kolom en het nummer van de regel.
A.R.A., 2e afdeling, archief Hugo van der Goes, inv.nr. 47; stukken betreffende J.A. de Vos van Steenwijk (nrs. 495 en 496); H.T. Colenbrander: *De Bataafse Republiek* (Amsterdam, 1908) p.213–216.
- [39] G.K. van Hogendorp: *Brieven en Gedenkschriften*(II) (’s Gravenhage, 1866) p.102, brief van G.K. van Hogendorp aan zijn moeder van 16 juni 1787. In 1789 stuurde de Nederlandse gezant in Engeland, A.W.C. Nagell, zijn gecodeerde brieven voor de stadhouder via prinses Wilhelmina. Zie hiervoor K.H.A., archief prinses Wilhelmina, inv.nr. 328, stuknrs 39 en 67. De bijbehorende code is te vinden in A.R.A., 2e afdeling, familiearchief Nagell, inv.nr. 123.

- [40] J. Naber: *Correspondentie van de Stadhouderlijke Familie*, deel 3 ('s Gravenhage, 1931–1937) p.180 voetnoot. Over de door de prinses gebruikte systemen is een artikel in voorbereiding.
- [41] M. Jahns: *Geschichte der Kriegswissenschaften vornehmlich in Deutschland*, deel 3 (München, 1891) p.1818, p.2636.