## CRYPTOANALYTISCHE VERKENNINGEN

# John Davys 1737

*Bron:* W.F. Friedman, *The Cryptanalyst Accepts A Challenge*
In *Articles on Cryptography and Cryptanalysis*
Reprinted from The Signal Corps Bulletin,
United States Government Printing Office, Washington, 1942.
Bewerkt door dr. Hans van der Meer 20 juli 2014

## 1 Cryptogram

In Londen in het jaar 1737 verscheen van de hand van John Davys het werk *An Essay on the Art of Decyphering*. Op blz. 32 daarvan valt het volgende te lezen:

> But, to make some Amends for the Letter, which I have *thus* intercepted, I shall supply its Place with Part of another, which cost me about four Hours close Attention to decypher, *Nov.* 5.1734. It is written in a very particular Manner, the like of which in some respects I have never seen. At the first View it strangely surprised me; I had before me a Prospect but of *cold Hunting*. And was *indeed* obliged *Consilium in arena capere, to take my Measures upon the Spot*. As the Case was new to me, so were my Observations upon it such as, I dare say, were never used before in the Business of decyphering. But they proved to be exactly right, and fully answered my Purpose.

*Extract of a Letter from the Earl of* Clanricard[1]
*to the Marquis of Ormond*[2]

90 6645737747 83576045 109 655383814976 34 99 677867767358495077 23 70577852 108 26 50495371 8378 36 435476415368 836977 22 40 59727860584153 68 39 764553 91 446577736975 78 30 5345735169 93 29 108 664568 43724176426957 105 22 104 32 8145795457836944 33 70577852 97 109 23 108 74495371 4269754569844582 34 61695175 93 5245 666083 24 824163458348 73 48658469 5378 20 5578854557 4970 49 72656045 111 21 105 40 106 7687 44608387 91 7041735972 30 8354 97 20 99 75785883 105 7669 30 91 111 576971606581686944 102 25 105 37 73 48418469 47787769 76606748 658259814163 105 38 5869457669 426083 22 50775485 39 111 617269574953 34 775481 61486583 24 6754845782 5978 83417469 25 91 666059 102 7663 6778777073446953 6745 7353 25 107 30 91 8169587945675982 39 8378 26

107 49 584854847544 102 69604557 80847359 83724958 36 847772657987 5049534744785245

This Extract now appears, just as it came to me, with two or three Errors in the Writing, as usual, and a few old Spellings, which I have not taken upon me to correct. I have produced this Piece, rather than some others now in my Hands, for the following Reasons.

- Because, as I have already intimated, it is a *Curiosity*.
- Because I am sure, that I have decyphered it right; for, some Time after I had returned it to Mr. *Carte*[3], he wrote me back Word, that he had found a misplaced Bit of Paper, by which it appeared, that my Interpretation was right to a Tittle.
- Because, being only a Fragment, and without Date, (tho *that* may nearly be discovered by the Contents,) it is not printed in Mr. *Carte*'s Collection.
- Because the same was afterwards decyphered by a very ingenious Woman, who is capable of becoming a great Proficient in the Art, as I also know several others of her Sex to be.

But the Truth is, that among those who are capable of the Work, very few are ∗ willing to undergo the Fatigue of it. Hence it is the less to be wondered at, that such strange Opinions have gone Abroad concerning an Art so little known. *Vieta*'s Performance was confidently given out to have been the Effect of *Magick*; and when *Locatello* published some *chymical* Secrets in Cypher, it looks as if he had the Fear of the *Holy Office* before his Eyes: For he takes especial Care to inform his Reader, that all those Passages (tho as yet only *written* in Cypher) had been explained to, and allowed by, his Superiors. So that now an innocent Preparation in *Chymistry* was secured from all Suspicion of *Heresie* or *Witchcraft*. However that were, the Generality of Men were not easily brought to believe, that a Writing might be decyphered by human Means; and I know not, wheter all are, even at this Day, convinced of it.

Tot zover het citaat uit John Davys' werk.

## 2 Cryptoanalyse

Het tijdstip is het begin van de 18e eeuw en dus beginnen we eerst maar aan een eenvoudig systeem te denken. De adellijke namen van de correspondenten doen vermoeden dat de tekst in het diplomatieke circuit moet worden geplaatst. Daarin heerste eeuwenlang de *nomenclatuur*. Aanvankelijk is dit een eenvoudige monoalfabetische substitutie, maar allengs wordt ze uitgebreid met equivalenten voor frequente letters (de homofonen) en met codegroepen voor lettergrepen, veelgebruikte woorden, uitdrukkingen, plaats- en eigennamen. Dit systeem nemen we als uitgangspunt voor onze onderzoeking.

Als eerste stap in de ontcijfering beperken we ons tot de groepen van vier of meer cijfers, omdat die wel woorden zullen voorstellen. Vervolgens zien we dat deze groepen *zonder uitzondering* een even aantal cijfers hebben. We kunnen daarom de volgende veronderstelling maken: de letters van het bericht zijn gecodeerd als dinomes[4]. De vrijstaande dinomes laten we bij gebrek aan beter voorlopig aan hun lot over. De eveneens vrijstaande trinomes[5] zouden codegroepen kunnen zijn.

| | | | | |
|---|---|---|---|---|
| 41 𝍸 III | 51 II | 61 III | 71 III | 81 𝍸 I |
| 42 III | 52 IIII | 62 | 72 𝍸 II | 82 𝍸 |
| 43 II | 53 𝍸 𝍸 II | 63 III | 73 𝍸 III | 83 𝍸 𝍸 𝍸 |
| 44 𝍸 II | 54 𝍸 II | 64 | 74 II | 84 𝍸 II |
| 45 𝍸 𝍸 𝍸 I | 55 I | 65 𝍸 III | 75 𝍸 | 85 II |
| 46 | 56 | 66 IIII | 76 𝍸 𝍸 | 86 |
| 47 III | 57 𝍸 𝍸 | 67 𝍸 II | 77 𝍸 IIII | 87 III |
| 48 𝍸 II | 58 𝍸 II | 68 IIII | 78 𝍸 𝍸 III | 88 |
| 49 𝍸 III | 59 𝍸 II | 69 𝍸 𝍸 𝍸 𝍸 I | 79 III | 89 |
| 50 IIII | 60 𝍸 𝍸 | 70 𝍸 | 80 I | 90 |

*Tabel 1 Telling van de dinomes in de woordgroepen.*

Eerst wordt een telling gemaakt van de dinomes in de veronderstelde woordgroepen. De getelde waarden lopen van 41 tot en met 87. Er is dus zeker geen sprake van een eenvoudige monoalfabetische substitutie met één dinome per letter. Voor meer inzicht in het systeem gaan we op zoek naar herhalingen. Onder de groepen met vier cijfers zien we 59 54 en 52 45 elk tweemaal voorkomen. Daarnaast zijn er ook bijna-herhalingen, zoals 48 65 84 69 en 48 41 84 69; deze verschillen slechts in één dinome. Staat hier misschien tweemaal hetzelfde woord? Kunnen 41 en 65 substituties voor een en dezelfde letter zijn?

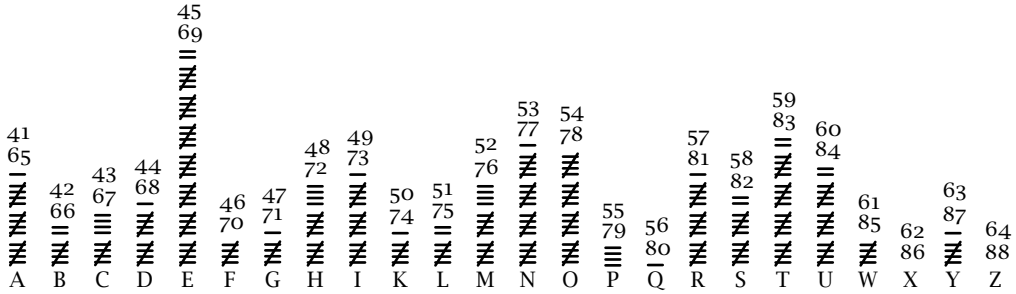
De gedachte dat 41 en 65 dezelfde letter voorstellen wordt nog aannemelijker als we naar het verschil van beide getallen kijken. Dat verschil van 24 is precies wat het aantal letters van het alfabet zou kunnen zijn. Bedenk dat in die tijd het alfabet minder letters telde dan nu. De U en de V waren nog niet gedifferentieerd en de J komt niet voor. Dit klopt ook redelijk met het feit dat we een traject van 47 verschillende dinomes vinden, namelijk 41–87. Tweemaal een 24-letter alfabet geeft natuurlijk 48 stuks, maar als de laatste letter zeldzaam is kunnen het er heel goed 47 zijn.

Onze werkhypothese luidt nu: er is sprake van twee parallel verlopende reeksen dinomes met tussen de reeksen een voor elke letter van de klare tekst constant verschil van 24. Deze hypothese laat zich met statistische technieken uitstekend evalueren. Daartoe testen we eerst de gepostuleerde reeksen 41–64 en 65–88 afzonderlijk op monoalfabeticiteit, om ze vervolgens met elkaar te vergelijken.

De *Index of Coincidence*[6] levert voor de eerste reeks de waarde $\varphi = 0.061$ en voor de

tweede $\varphi = 0.060$. Daarmee is het monoalfabetisch karakter van de beide reeksen wel afdoende aangetoond. Vervolgens bezien we in hoeverre de beide reeksen precies parallel verlopen. Daarvoor leent de $\chi$-*test*[7] zich. De gevonden waarde $\chi = 0.061$ past wederom uitstekend bij de werkhypothese.

Nu de relatie tussen beide reeksen is vastgesteld, kunnen ze worden gecombineerd. Voor frequentieverdeling van de gecombineerde reeksen wordt de alleszins bevredigende waarde van $\varphi = 0.077$ berekend. Invullen in het cryptogram brengt meteen een flink aantal herhalingen aan het licht. Verder zien we aan de hoge frequentie van het paar 45 69 dat dit wel de letter *e* zal zijn. Ook zien we zonder veel moeite in 53 77 en 59 83 de letters *n* en *t* komen. Nu is 83 78 natuurlijk *to*, hetgeen voor 54 en 78 de letter *o* oplevert. Zo kunnen we doorgaan, maar het is nuttiger om de gecombineerde frequenties eens goed aan te zien.




*Tabel 2 De reeksen 41–64 en 65–88 gecombineerd.*

De gecombineerde telling in tabel 2 vertoont onmiskenbaar de trekken van de normale verdeling van de letters over het alfabet. Getuige bijvoorbeeld het plateau van de groep r,s,t,u met daarvoor de kuil van p,q alsook de kuil van w,x,y,z aan het eind van het alfabet.

## 3 Ontcijfering

Het merendeel van het cryptogram kan nu worden ontcijferd. Als we het woord *cocmisikn* zien optreden, hebben we een van de door Davys genoemde vercijferfouten te pakken. Dit moet natuurlijk *commission* zijn. De *c* is 67, de *m* is 76: de cijfers van de dinome zijn kennelijk omgewisseld.

| | | | |
|---|---|---|---|
| 90 = although | 96 = ? | 102 = for | 108 = H.M. |
| 91 = and | 97 = England | 103 = ? | 109 = that |
| 92 = ? | 98 = ? | 104 = is | 110 = ? |
| 93 = of | 99 = has | 105 = it | 111 = not |
| 94 = ? | 100 = ? | 106 = just | |
| 95 = ? | 101 = ? | 107 = the King | |

*Tabel 3 Toekenning van de codegroepen.*

De losse dinomes met lage waarden blijken loze groepen. Zie bijvoorbeeld het fragment „ten 22 40 thousand 39 men". De afzonderlijke cijfergroepen van 90 tot en met 111 kunnen echter niet worden gemist. Deze ontpoppen zich – zoals al werd verondersteld – tot codegroepen. De betekenis van deze codegroepen moet worden bepaald uit de context van het bericht. Als voorbeeld nemen we „king beleeves well 93 me". Dit kan worden gelezen als „king beleeves well of me". Aan de groep 93 wordt de betekenis *of* toegekend. Het is niet eenvoudig om alle codegroepen van een goede betekenis te voorzien. De toekenning in figuur 3 is van de hand van William Friedman. Deze toekenning is gebruikt in de navolgende klare tekst van het bericht.

> although being true that Antrim[8] has commission from H.M. King[9] to comand ten thousand men and Daniel O Neile[10] of H.M. bed chamber it is reported from England that H.M. King beleeves well of me but sayeth I have no power if I have not it just my duty and faith to England have lost it me and not reguarded for it I have gone much astray it seems but know not wherin nor what cours to take and but for my confidence in the King and respects to the King I should for ever quit this unhapy kingdome

---

[1] Clanricarde is een Ierse titel behorend bij een gebied in County Galway. Hier is vermoedelijk bedoeld Richard Burke (†1666), de 6e Earl of Clanricarde. Hij was gehuwd met Elizabeth Butler, de dochter van Walter Butler (1569–1632/3), de 11e Earl of Ormond.

[2] Ormond is de titel van de Butler familie met bezittingen in de huidige counties van Tipperary, Kilkenny en delen van County Carlow. Walter Butler werd opgevolgd door zijn kleinzoon James (1610–1688) de 1e Hertog van Ormonde en van 1642–1661 Marquess of Ormonde. Leefde met Karel II in ballingschap in Europa en werd na diens restauratie in 1660 een van de leidende figuren in de Engelse en Ierse politiek. Dit is ongetwijfeld de geadresseerde van deze brief.

[3] Bedoeld is Thomas Carte (alias John Carte) (1686–1754), een Engels historicus die o.a. een driedelige studie schreef getiteld *Life of James Duke of Ormonde*, Oxford 1735–1736.

[4] Een dinome is groep van twee cijfers.

[5] Een trinome is groep van drie cijfers.

[6] De Index of Coincidence wordt gegeven door de formule $\frac{\varphi=\sum_{i=1}^{n} f_i(f_i-1)}{/N(N-1)}$ waarin $f_i$ het aantal letters $i$, $n$ het aantal letters in het gebruikte alfabet en $N$ het aantal letters in het cryptogram.

[7] De *chi*-test wordt gegeven door de formule $\frac{\chi=\sum_{i=1}^{n} f_{1i}f_{2i}}{/N_1N_2}$ waarin $f_{1i}, f_{2i}$ het aantal letters $i$ in de respectievelijke distributies en $N_1, N_2$ de overeenkomstige totalen.

[8] Antrim is een van de counties van Noord ierland. Waarschijnlijk wordt hier bedoeld Randal MacDonnell, 1st Marquess of Antrim (1609–1683). Aangezien hij van juli 1660 tot mei 1661 in de Tower van Londen is vastgehouden op verdenking van verraad, maar daarna zonder beschuldiging werd vrijgelaten, zou dit deze brief na mei 1661 dateren.

[9] Karel II van Engeland.

[10] Dit moet de Ierse Daniel O'Neill (c.1612–1664) zijn. Bij de restauratie van Karel II in 1660 werd hij voor zijn steun beloond met een groot aantal functies en werd als gevolg daarvan een van Engelands rijkste mannen. Gezien zijn overlijden op 24 oktober 1664, begrenst dit deze brief tot uiterlijk die datum.