

PRACTICUMBOEK CRYPTOGRAFIE

Informatica en andere bètastudies

dr. H. van der Meer



EDITIE 2015

© dr. H. van der Meer, 2015. Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotocopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming.

Inhoud

1	Inleiding	1
1.1	Algemene informatie	1
1.2	Programma van eisen	1
1.3	Practicum	2
1.4	Tentamen	3
2	Transpositie	7
2.1	PRACTICUM – Transpositie oplossen	7
2.2	BONUS – Routetranspositie	10
2.3	BONUS – Kolommen van gelijke lengte	10
2.4	BONUS – Kolommen van verschillende lengte	11
2.5	BONUS – Paren met eenzelfde begin of einde	11
2.6	BONUS – US Army Double Transposition	12
2.7	BONUS – Onregelmatige kolommen	12
3	Monoalfabetische substitutie	17
3.1	PRACTICUM – Monoalfabeet oplossen	17
3.2	BONUS – Cryptogrammen met woordverdeling	18
3.3	BONUS – Cryptogrammen zonder woordverdeling	22
3.4	BONUS – Cryptogrammen in andere taal dan Engels	23
4	Polyalfabetische substitutie	27
4.1	PRACTICUM – Porta oplossen	27
4.2	PRACTICUM – Beaufort oplossen	30
4.3	BONUS – Porta normaal alfabet	31
4.4	BONUS – Vigenère normaal alfabet	31
4.5	BONUS – Beaufort normaal alfabet	32
4.6	BONUS – Vigenère met gemengd alfabet	33
4.7	BONUS – Isologe cryptogrammen	35
5	PRACTICUM – Oververcijfering oplossen	39
5.1	Slag by Midway	39
5.2	Systeem van vercijfering	39
5.3	Cryptogrammen	40
5.4	Werkschemas	42

6	PRACTICUM – Alfabet reconstructie	49
7	PRACTICUM – Kerckhoffs superpositie oplossen	51
8	PRACTICUM – Hagelin oplossen	55
9	WEDSTRIJD – Uitdagende opgaven	67
9.1	Kies een opdracht	67
9.2	Drugs oefening *	68
9.3	Normandië oefening **	72
9.4	Pearl Harbour oefening ***	85
9.5	Noord Afrika oefening *****	95
A	Tabellen	105

Hoofdstuk 1

Inleiding

1.1 Algemene informatie

- *Actuele informatie*

Op de website wordt actuele informatie over het lopend college verschaft. Het belangrijkste hiervan is het tijdschema voor de behandeling van de stof. Benut dit om de colleges voor te bereiden. Hier vindt men ook materiaal dat kan worden gedownload.

Website URL = <https://staff.fnwi.uva.nl/h.vandermeer>

Website URL = <http://hvdmeer.myqnapcloud.com>

Het UVA-Blackboard systeem wordt niet gebruikt.

- *Beschikbaarheid van de docent*

De docent is al geruime tijd met pensioen. Het gevolg is een beduidend verminderde beschikbaarheid voor het beantwoorden van vragen en het helpen bij problemen anders dan tijdens de geroosterde contacturen. Dit is buiten de collegeperiode zeker het geval. Aanbevolen wordt deswege om meteen de eerste tentamengelegenheid te benutten en het niet op het hertentamen te laten aankomen.

- *Tentamen*

Een aantal tentamenopgaven is hierachter opgenomen en is bedoeld om een indruk te geven van het soort vragen. Het werkelijke tentamen kan (en zal) natuurlijk afwijken.

- *Leeswijzer*

In de syllabus voor studenten Informatica en andere betastudies behoren de gedeelten met een donkerder bladspiegel niet tot de verplichte stof. Deze zogenaamde mastersecties gaan dieper op het onderwerp in en zijn bedoeld voor studenten die meer over het onderwerp willen weten. In het tentamen worden daarover geen vragen gesteld.

1.2 Programma van eisen

- *Inleiding*

Kunnen uitleggen van basisbegrippen uit de cryptografie: veilig en onveilig kanaal, verschil klassiek en publickey systeem, principe van de quantumcryptografie, soorten aanvallen op geheimschrift, eigenschappen zoals endomorfie, idempotent, gelijksoortigheid, restklassen, enz.

- *Klassieke systemen*

Een beschrijving kunnen geven van de in de syllabus behandelde geheimschriften. Zoals transposities, monoalfabetische en polyalfabetische substitutie in diverse vormen, codes, enz. In die geheimschriften een bericht kunnen vercijferen en ontcijferen. Er zal geen *echte* cryptoanalyse worden gevraagd. Kunnen beschrijven van behandelde cryptografische apparatuur zoals Wheatstone, Hagelin, Enigma, Purple. Constructie uit een sleutelwoord van sleutels voor transpositie en substitutie.

- *Cryptoanalyse*

De berekening en het gebruik van het tweede moment van een symbooldistributie in de cryptoanalyse kunnen behandelen; bijvoorbeeld voor de bepaling van monoalfabetischeit en de periode van polyalfabeten. Coïncidenties en chitest voor het matchen van letterdistributies. Het verschijnsel isomorfie en toepassing ervan bij de reconstructie van het cijferalfabet, decimatie van het alfabet.

- *Informatietheorie*

Kunnen uitleggen van de grondbegrippen entropie en equivocatie. Het belang van Markov ketens voor de cryptografie, redundantie in natuurlijke taal, uniciteitsafstand en de betekenis daarvan voor de cryptoanalyse. In het bijzonder voor studenten Informatica en andere betastudies: binair symmetrisch kanaal in relatie tot het one time pad systeem. Over deze zaken kwalitatief kunnen redeneren en voor een eenvoudig informatiekanaal berekening van de equivocatie kunnen uitvoeren.

- *Moderne systemen*

Goede beschrijvingen kunnen geven van het Feistel schema, de Data Encryption Standard en de Advanced Encryption Standard. Een globale beschrijving kunnen geven van de andere behandelde systemen. Iets kunnen vertellen over de cryptoanalyse van deze systemen, voorzover behandeld.

- *Openbare sleutelsystemen*

Grondslagen kunnen uitleggen en redelijk gedetailleerd de op college behandelde systemen kunnen beschrijven, waaronder in ieder geval RSA, ElGamal en de Diffie-Hellman sleuteluitwisseling. Kunnen aangeven op welke wiskundige grondslagen deze systemen berusten. Zaken van belang m.b.t. de keuze van de systeemparameters, de gebruikte priemgetallen, toepassing van elliptische krommen. Discrete wiskundesommen worden niet gevraagd.

- *Sleutelstroom*

Bekendheid met het principe van Vernam-vercijfering, periodiciteit en kwaliteit van pseudorandom bitrijen. Werking, karakteristiek polynoom, periodiciteit en samenhang met de behandelde schuifregisters kennen. Combinaties van schuifregisters zoals Multiplex, Geffe, Pless, A5 gsm-vercijfering en de andere behandelde schakelingen kunnen beschrijven. De terugkoppelfunctie kunnen bepalen uit een productietabel. In globale termen de correlatie-aanval kunnen beschrijven.

1.3 Practicum

- *Practicum cryptoanalyse*

Meedoen aan de klassikale opdrachten tijdens de colleges spreekt uiteraard vanzelf. Het verdient aanbeveling om bij het oplossen op het practicum een potlood te gebruiken en een vlakgum bij de hand te houden. Met ballpoint of pen wordt het gegarandeerd een onleesbare knoeiboel. Op de website kan men zien wanneer welke practicumopgaven zullen worden gedaan. Lees vooral de toelichting in het werkboek aandachtig, dat scheelt aanzienlijk in het werk.

- *Bonusopgaven*

Het inleveren van practicumopgaven is geen voorwaarde voor deelname aan het tentamen. Het is verstandig om een beschrijving van het eigen oploswerk mee in te leveren – ook als de oplossing zelf niet is gevonden of foutief lijkt – omdat dit toch een positieve invloed kan hebben. Succesvol inleveren van practicumopgaven leidt, afhankelijk van aantal en kwaliteit van de ingeleverde oplossingen tot een bonus in het tentamencijfer; het oordeel van de docent is hierin doorslaggevend. Inleveren van de oplossingen uiterlijk bij de eerste tentamengelegenheid.

- *Wedstrijdopgaven*

Het practicumboek bevat een hoofdstuk met een aantal grotere cryptoanalyseopgaven. Deze zijn bedoeld als uitdaging voor diegenen die cryptoanalyse leuk zijn gaan vinden, bij zichzelf aanleg daarvoor hebben ontdekt en, last but not least, er de tijd voor kunnen vrijmaken zonder de rest van hun studieprogramma in gevaar te brengen. De opgaven zijn van verschillende zwaarte, hoe meer sterren hoe moeilijker. Het is toegestaan om met een team van maximaal twee personen zo'n opgave aan te pakken. Een team kan slechts één oplossing inzenden. Bij elke collegecyclus zal een deadline voor inlevering worden aangegeven. De ingeleverde opdracht moet behalve de oplossingen van de cryptogrammen ook een verslag van de wijze van oplossen bevatten. Voor de eerste goede oplossing in elke categorie wordt een prijs ter beschikking gesteld; deze varieert met het aantal sterren van de opgave. De wedstrijdopgaven zijn niet triviaal gebleken, want in de afgelopen decennia zijn maar enkelen er in geslaagd een prijs te behalen. De cryptogrammen voor deze opgaven kunnen vanaf de website worden gedownload.

1.4 Tentamen

In de cursus 2012–2013 is voor het toetsen van kennis van de stof geëxperimenteerd met een component van multiplechoice en andere korte vragen. Dit wordt voortgezet.

Opgave-1

1. Maak een 5x5-sleutelvierkant met sleutel EXEMPLARISCH. Laat de J weg. Label de rijen en kolommen met de letters ADFGX. In de vercijfering komt eerst de rij- dan de kolomcoördinaat.
2. Vercijfer met dit sleutelvierkant de volgende tekst (rijcoördinaat eerst, spatie tussen opvolgende lettercoderingen):
DE YANKEES KOMEN FRANSEN JUICHEN DUITSERS HUILEN
3. Maak een transpositiesleutel met behulp van de sleutel CHEMIN DES DAMES.
4. Vercijfer met de zojuist gemaakte sleutel de eerder verkregen substitutie door middel van een kolomtranspositie. Presenteer het cryptogram zoals het hoort.

Opgave-2 Geef een beschrijving van de cryptografische rotor. Wat is het effect van het aan elkaar koppelen van rotors?

Opgave-3

1. Wat betekent het *commuteren* van twee cryptotransformaties?

2. Waarom zal men bij het combineren van verschillende cryptotransformaties tot een samengesteld cryptosysteem commuterende basistransformaties vermijden?

Opgave-4

1. Leg uit hoe langs statistische weg de periode van een polyalfabeet kan worden bepaald.
2. Hoe heet de bij deze methode gebruikte statistische grootheid en hoe is deze gedefinieerd?

Opgave-5 De regel van Bayes toegepast op een systeem met berichten M , cryptogrammen C en sleutels K geeft als de voorwaardelijke kans op een bericht M gegeven een bericht C :

$$P(M|C) = P(M)P(C|M)/P(C)$$

Beschrijf in woorden wat dit betekent en laat zien onder welke omstandigheden de best mogelijke veiligheid wordt bereikt. Geef ook aan wat dit betekent voor het aantal sleutels in sleutelverzameling K .

Opgave-6

1. Waarop berust de grootheid *entropie*? Geef de bijbehorende formule voor de berekening ervan.
2. Wanneer sprake is van twee samenhangende gebeurtenissen i en j , afkomstig uit respectievelijk de verzamelingen I en J , is er een kans p_{ji} dat gebeurtenis j wordt aangetroffen in vervolg op gebeurtenis i . Gegeven dat de kans op het optreden van i de waarde p_i heeft, laat dan zien hoe de informatie-inhoud van het totale systeem kan worden bepaald. Hoe noemt men de grootheid die de *interactie* tussen de beide gebeurtenissen vastlegt?

Opgave-7

Geef een gedetailleerde beschrijving van de *rondetransformatie* in de Data Encryption Standard (DES).

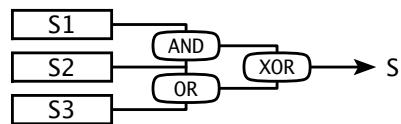
Opgave-8 Geef een beschrijving van het knapzakstelsel. Waarop berust het stelsel, welke zijn de parameters, hoe wordt gecijferd en ontcijferd.

Opgave-9

1. Teken het verbindingsschema van de terugkoppelfunctie behorend bij een lineair schuifregister met als karakteristieke functie
$$f(x) = 1 + x^2 + x^3 + x^4 + x^8$$
2. Aan welke eis moet een terugkoppelfunctie voldoen om een maximaalrij te genereren?
3. Hoe groot is de periode van een maximaalrij? Verklaar ook kort waarom.
4. Verklaar waarom een maximaalrij voldoet aan het 3e criterium van Golomb.

Opgave-10

1. Werk de productietabel uit voor de sleutelstroom van de in de figuur gegeven combinatie van drie schuifregisters.



2. Bepaal de terugkoppelfunctie behorend bij deze sleutelstroom in algebraïsche normaalvorm.
3. Bereken de correlatie tussen de uitvoerstroom en elk van de drie samenstellende schuifregisters.

Hoofdstuk 2

Transpositie

2.1 PRACTICUM – Transpositie oplossen

Hieronder staan twee cryptogrammen die een enkelvoudige kolomtranspositie met dezelfde sleutel hebben ondergaan. Bekend is dat deze twee cryptogrammen hetzelfde slot hebben. De opgave is om deze twee cryptogrammen te breken. We zullen de cryptoanalyse stap voor stap opzetten.

PRACTICUM-1 Engels (eindigen hetzelfde)

ETRTE EESOA AEUNI VAFLN IAMND RYHRV MENRI EETRO UDCCC OHTCY MRREA
RHITN DEYEN RNERV SRBEN IGSKA ILNRA NFNAD ALOLT XOMAH HRREI

TLVSX OPNRE MEFDS KYENR UEERB TSREH TIAN TIVYMR VESIR EENEI NOLTM
NNEDE TROOP UNARA CIAAI NSCWN A

1. Het begint met het uitzoeken waar kolommen beginnen en eindigen. Omdat de twee cryptogrammen dezelfde tekst aan het eind hebben staan, zullen de laatste letter(s) van elke kolom in beide cryptogrammen (aaneensluitend) voorkomen. Als een en ander niet duidelijk is, maak dan zelf een voorbeeld door twee klaarteksten met een flink lang gemeenschappelijk slot te vercijferen en de overeenkomsten tussen de beide cryptogrammen op te merken.
2. Onbekend is natuurlijk om hoeveel gemeenschappelijke letters het gaat, want dat is afhankelijk van de lengte van de gemeenschappelijke tekst. Het helpt echter als we bedenken dat de laatste letters van elk cryptogram ook tevens de laatste letters van een kolom zijn.
3. Daarom beginnen we aan het eind van elk cryptogram en gaan als volgt te werk. Het eerste cryptogram eindigt op `..RREI`. We hebben vier letters opgenomen, zodat het aantal onderzochte letters niet te klein is; we zien wel hoeveel letters er straks van overblijven of dat het fragment zelfs nog te kort is. We bekijken alle groepjes letters in het tweede cryptogram die op `I` eindigen.

ETRTEEESOA AEUNIVAFLN IAMNDRYHRV MENRIEETRO UDCCCOHTCY MRREARHITN DEYENRNERV SRBENIGSKA ILNRRANFNAD ALOLT XOMAHHRREI
--

TLVSXOPNRE MEFDSKYENR UEERBTSREH TIAN TIVYMR VESIREENEI NOLTMNNEDE TROOPUNARA CIAAINSCWNA
--

4. We vinden `..EHTI..`, `..ANTI..`, `..VESI..`, `..ENEI..`, `..RACI..`, `..IAAI`. Als het gemeenschappelijke stuk tekst zo kort is dat maar één letter in elke kolom overeenkomt, dan hebben we pech en moeten we al deze posities stuk voor stuk onderzoeken. Er

is echter één positie waar twee letters overeenkomen, namelijk de laatste twee letters van het groepje . . ENEI . . . In het vertrouwen dat dit misschien wel goed is noteren we dit veronderstelde kolomeinde in bijgaand schema door boven de betreffende letters een streep te zetten. Als dit inderdaad de twee gemeenschappelijke laatste letters van een kolom zijn, mogen we voor de lengte van de andere gemeenschappelijke stukken concluderen tot: hetzij 1 à 2 letters overlap, hetzij 2 à 3 (bedenk zelf waarom dit zo is). Laten we hopen dat het 2 en 3 zullen blijken te zijn.

5. Herhaal de procedure met de laatste letters van het tweede cryptogram. Daarna is er geen hulp meer van een vast kolomeinde en moeten we geheel op eigen kracht verder. Een goede strategie is om van het eind van een kolom naar voren te gaan en de op-eenvolgende letters te vergelijken met die in het andere cryptogram. Op een gegeven moment wordt wel duidelijk hoe lang de kolommen in elk van beide cryptogrammen zijn. Denk erom dat in dit systeem niet alle kolommen van een cryptogram dezelfde lengte hebben. Ga door tot beide cryptogrammen compleet zijn opgedeeld. Het aantal gevonden kolommen levert meteen ook de lengte van de transpositiesleutel.
6. Aangezien korte en lange kolommen hooguit één letter in lengte kunnen verschillen en omdat beide cryptogrammen dezelfde sleutel, en dus evenveel kolommen hebben, kan er het een en ander aan gerekend worden. Op die manier is het mogelijk om een veronderstelde kolomlengte of een veronderstelde sleutellengte te testen op consistentie tussen de twee cryptogrammen.
7. Pas op. Er is één punt in de opdeling waar het vinden van het eind van de eerste en het begin van de volgende kolom lastig is. Het is wel cruciaal voor de volgende fase van de analyse om dit goed te doen. Als bij het anagrammeren problemen ontstaan en er maar geen goede klaartekst wil komen, is dat de waarschijnlijke oorzaak. Waar de schoen wringt is vanzelf wel duidelijk als het probleem zich voordoet.
8. Als de opdeling in kolommen gevonden is, schrijven we deze kolommen uit in de linkerhelft van het werkschema. De eerste vier letters van elk cryptogram (natuurlijk tegelijk ook het begin van een kolom) zijn reeds ingevuld. Het invulschema aan de rechterkant is bestemd voor de door anagrammeren in volgorde geplaatste kolommen. De bovenste regel is voor het kolomnummer. Anagrammeer beide cryptogrammen simultaan totdat de oplossing compleet is. Let op. Het aantal rijen en kolommen in het werkschema is niet gelijk aan het werkelijke aantal rijen en kolommen, want dat zou al te gemakkelijk zijn.

WERKSCHEMA

0 0 0 0 0 0 0 0 0 1 1 1 1 1 1
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5

E

T

R

T

.

.

.

.

.

.

.

.

T

L

V

S

.

.

.

.

.

.

.

2.2 BONUS – Routetranspositie

Probeer een aantal standaard routes om de juiste volgorde te vinden.

ROUTE-1 Engels

LEOCO ADPIG HHNSI NAGWI IUNLO TDGTV HOLES MYHSF DRARN OSIEI EANVV
OUNEE GSTEN NPNAB EC

ROUTE-2 Engels

ATRVF MHCYT EMOTT CTMHS ORSEE HOEMN ENEIP SXNTM FPTIO OETX

ROUTE-3 Engels

KSHOF IREHI UYLBS ENTWE RYLKG ASIOI GTLTS UEHHK RTSTS RIYET HOONX
SLIMU

2.3 BONUS – Kolommen van gelijke lengte

Probeer kolomlengtes die een gehele deler zijn van het aantal letters in het cryptogram. Begin met de lengte(s), die op grond van het aantal klinkers in elke rij, het meest waarschijnlijk zijn.

KOLOM-1 Engels

UEERH ERTAE IHATA LXEKL STTYP GLIZO EAHRM MEISO OCLGF ETTIO ZRPAT
ONTON NEOLT N

KOLOM-2 Engels (bevat woord: exist)

NDBEA ENATD VXSFA RRASC ATIDE HSMTK MESOT LCTLO MCYHS WSSTI USSOY
SISEX DSETF SFOBO EAE OV TOBAR RNXNA EKNBN ORCNL ENEAB HBPSS KVIDM
COEOH TEIAD

KOLOM-3 Engels (kolommen zijn lang)

VEDEJ OBEEN MTOVE LOHxD WRUOE THBSS WTEDS IVTLE NRSGR OIORU ANEBR
RMEYO LTWTT DIEOK HETGI AAROR UFUCD MORRA MLAEP RRPBI TEGNV VRCTC
NEREA RETYT SSUOO YZDLI TTICE TERSY ELITB OAEWN ES

KOLOM-4 Engels

van: Engels (Nihilist, Caesar aanwijzing: NYWX)

TPNIR HMSBS ENROI TIEMH KTOJS YEEAT TUUET HXNTH OLMRL EATRE AOMYK
AYAKW ADES

2.4 BONUS – Kolommen van verschillende lengte

KOLOM-5 Engels (heeft 7 kolommen, bevat woord: dwelling)

WIRMN NATUE IEAWS HESAD DHEME EIESN NEESN TEIBN TFOHR TREII HDLEA
VREM N LEYEU HRLTM RETTN ERFUE TERXN SDGTR EOGAR CYEGI CWASE CLHTE
LRHED DERII AEHGO WWHEP FTRUH R

KOLOM-6 Engels (heeft 18 kolommen)

EPAHR ELNFO CPOIO ASROS MWIWA SOTAV TIOES INDED DXTAT YTN TU OMECP
ASFCR LTORN MOGRA SAORO SLLAH AMGAB OGTEW DOSME ILOOO DRFTA TVABT
RHDER DEXPH NOYIP WIITO CEDON WIRTU LMRNX LWAIN OVTUH LIONN XARLU
SOTSS RNNMI EGERH AATCE FRMOS NS

KOLOM-7 Engels (bevat woord: ammunition)

UIMYN LLKNM SYITE ESEPN IQNNA FPEGD OSUUT SIPCE ANROW NETCU ETPIE
ETEAT LUOPS BSOLE STMTE NEHNO HREIL TRVBD SOYNP

2.5 BONUS – Paren met eenzelfde begin of einde

Bepaal aan de hand van de overeenkomstige letters het aantal kolommen, splits de cryptogrammen vervolgens in kolommen en los op.

KOLOM-8 Engels (beginnen hetzelfde)

BNTSE ARKCL CETTN BITER ROTAE LTNNO NNENO OTOKM SZTGN YITDK LANAE
FTFSN PGNPA RWOIA OFGTF CTOTD NINOE WXERF ASIOS TIDRR RMMAO ARPAT
OUTIO BIEOA GAAPN EIK

BNTSE INDOT LCETS AFPLE RROMO ISOEN NONST IIUTO KMFY KPCYI TDVSI
NTAEF TFSTO NTNAR WOARO EEKTF CTTLT AEANO EWXPV TITIO STTTF OCMMA
OOSCA NROUT IEELS OAGAA ABITR T

2.6 BONUS – US Army Double Transposition

DOUBLE-1 Engels (zelfde sleutel 3 berichten)

RJETU EBDIT TLVTR IRYCN EORHN EATSI OOSTF CTDDR VFEAY MSNLD EOXER
 EHPYR UIEIE PIEMN AO
 NTEIT EROML CNANC INUCM LELAE NLASP OAMSE LTEON RTVOL TRITI YAXWT
 IEHSN EEFPR SPFII IS
 AQELE EYDS EAEAN CMNAU ONCND AICRG NRGNA ERTEA BCIPH ERTNC ATTAC
 USALN DTUHE IRPWM VB

DOUBLE-2 Engels (zelfde sleutel 5 berichten)

IAALN EOFSG TOGVE RANOL NDUOD EIHIS ATFTD NRLVO RODSW EEROR Q
 TDNMR GREON ARIEU ETNYI TCOFE AIEUT TARDT EDNSO EIPEC MFEAR N
 ANELN EXEHG ILACE MEENL FXTEE EISIG AORWL LDLVV ORDEL OCHOT H
 EENET SLNNF TCOID OSEAI LFIGD WIAAR NOIHN LLNRF VWLRE MRAIE A
 RAMET MIONO DIUMA LLINX OATGT NNAIB TNHIT NIASD RMSEC UIOVS A

2.7 BONUS – Onregelmatige kolommen

De navolgende cryptogrammen komen uit de Zendia-oefening. Dit is een uit de Amerikaanse legeropleiding stammende opgave met 375 cryptogrammen in vele cryptosystemen. De transposities in deze oefening hebben een transpositieblok dat er uit ziet als een kruiswoordpuzzel: een deel van de vakjes is zwartgemaakt en kan niet met een letter worden gevuld. Aldus ontstaan kolommen van wisselende lengte die niet zomaar naast elkaar gelegd kunnen worden. Gegeven de aard van de oefening (een dag uit de campagne van het leger van Zendia tegen een Amerikaanse invasiemacht) mag in de teksten een militair jargon worden verwacht.

De transpositie-berichten kunnen worden verdeeld in drie groepen, elke groep correspondeert met een ander transpositieschema. Deze drie groepen worden elk aangeduid met een zogenaamde *discriminant*: ECHCE, GIFIG, JAAAJ.

De eenheden van het leger van Zendia zijn verdeeld over communicatienetwerken. In elk netwerk kunnen meerdere stations actief zijn. De stations worden van elkaar onderscheiden door een (dagelijks wisselende) drie-letter combinatie, het *call-sign* van het station.

Een paar opmerkingen bij de presentatie van de berichten. In de bovenste regel staan de gegevens van het onderscheppend af luisterstation. Met MKP DE PSD wordt aangegeven dat het bericht afkomstig is van station PSD en bestemd voor MKP. Verdere gegevens van het onderschepte bericht op deze regel zijn: tijd, radiofrequentie en intern volgnummer (USM kan worden gelezen als United States Marines). De datum van onderschepping is 23 december.

De tweede regel bevat een reeks cijfers. Daarin heeft de afzender een aantal gegevens gecodeerd: het volgnummer van alle van dit station uitgaande berichten, een apart volgnummer voor deze specifieke communicatielink, de prioriteitsklasse van het bericht en nog enkele meer.

Het bericht zelf begint na de eerste groep op de volgende regel. Deze eerste groep is de discriminant van het gebruikte cryptosysteem. Aan het eind van het bericht worden de twee eerste groepen herhaald. Berichten mogen niet te lang zijn en worden daarom zonodig in delen opgesplitst.

ZENDIA/ECHCE-1 Engels (bericht #010)

MKP DE PSD 2960KCS 230053T USM-99/00010

5518 4823 0010 5504 1476 6607 5762 6107

ECHCE TNUOS ROIRT APDIU XRDOA EMPAN ENERO CSRUC SSOQF LOCNN RPOTL
FIEEA ETIEN NSHNP GSSPO ETOTE NAFYR AAWSI RUJLS EMRII EAOPA HRHTA
ROECO AMSIN RRHOP ELINT LMNME UEZAB EDATO FARLT PCOOZ OEATR RCEEQ
RPPAU ENEAE SEMPA BLPEB ONFSR TDEZT OUNNS NETER EIREE MAEXI MMTIB
LNLDO OASRS MLPOE LOSMC NRORP PONO A EVRXB ACTMF NENEF ESNEP EIAIA
CGOXO UYCNM MAELL AWVED ECHCE TNUOS

ZENDIA/ECHCE-2 Engels (bericht #011)

MKP DE PSD 2960KCS 230114T USM-99/00011

5528 4823 0010 5504 1476 6607 5762 7516

ECHCE TWMUO NOMZT APVLL NEROA OSMCP ERECE NSIDO ZSTMO WECUE RPORU
SEZEA ETHEI AROZP GSTPM AROTO FTPNI NOWSA RAIMZ EMREE ELORO EPCEP
ONOSO EABTM NUXOI UNNIM MEDRH XAAVE AUMNE SSECR FPPAO FOPOX SEMEU
OAMBO TLMTW MARAE RELRE GERNO OEDTA PRRTD HPILP RTXTC MVCZM IUECR
OECNT ERBTO GRSSR ENPRN AISON OIRNE MVNPC PAZAO OADEE LMTPC WTLA
MHOLT ERTEE EOEXO HUEII EAAAZ ESARK GVITC XSWOP PSRER ASACI RRPIB
EANAT RNELN EESAP EZCGF UMPEE ACEKO MOTEA ECHCE TWMUO

ZENDIA/ECHCE-3 Engels (bericht #089)

MKP DE PSD 6760KCS 230708T USM-99/00089

5558 5123 0600 0121 4257 6607 5762 5429

ECHCE RNNNS RESPE EETMO VEECA AOCOI RODRU UZNVE TTEIE IBNNO MIFOM
SINTM LTDRB EFIOO TNNON XNMTD ELEIE FEEHA POAOU RNUQK AEEBD OCBAN
IPOUI AAISE EEDAI YTIUH TSTTO KOALM NONDC LLTSN AVESO KDTNT LROAT
TSAAP LCLKR ARTAE FOPNI OOCFY PKEOS TNCNS TNUDI GHCRI TDDNO UFICN
EDEAX SSSNT IANIT LEALE ALPPS RIICD QOIEO IENTP ECHCE RNNNS

ZENDIA/ECHCE-4 Engels (bericht # 179)

MKP DE GKW 6100KCS 231142T USM-99/00179

3518 2423 1110 4775 7046 9893 5762 3332

ECHCE RAFNO EAI0I MMTEL OLFFY GDWCO SAGBX DENCU UTSRI WBHTP RRUSD
LFBNR UNEAO EOAE EVOG NTRSE NTMCA TTEOI ETRNO PNEIE COEO RVFIX
RRHWN NETTP T000I OEEEE STZZA RTETD URFWP NOION AOWO ECHCE RAFNO

ZENDIA/ECHCE-5 Engels (bericht # 250)

GKW DE MKP 7320KCS 230925T USM-99/00250

2035 9123 0620 5504 3456 6625 9399 4811

ECHCE OIQHR LUATR RHAHM EPPDV GSCNT NNCER ETDOL SEHDT ILCMF SFRTT
TIEYR DERDE NRRTE EHATE EYMA SDAOR OARIU IEEMA AEOET AYSEE EUBER
ELSIB OMHQI PROUB RTESP DLMAA GAHBE XEODD ETLEI DSMRD SDENE ROOW
SEHER ECFAO ETBYN RHRAL RWCME DHRPO LYFWI UTIEE CRNOT PHDTO OOBXI
ARTEE EETSV ECHCE OIQHR

ZENDIA/ECHCE-6 Engels (bericht # 335)

HZY DE MKP 3440KCS 232057T USM-99/00335

5066 2623 1830 1120 7263 6625 6473 7014

ECHCE FOAOS MBEDN CNHII XRSRO NVNNR ESSTM CCNRE LELNT EMTPU AEIOH
GEEET DAEED NYPRS NMCTI LDAEE OLOO COICN RIAET ADHFI SSPIU TREGD
MIMCA UHDAD TPEOE OETA EAEIE ILREE EXELN EOWMT ANEEP AAODM SVRAN
TITLM SFAOL DSLBC INCSI SACC DSML ENMBL LEKLF CAIAA ROPOE OCWIA
OEIE TNNCE EDIOO LADIN ECRDM MTHSC VNGNA GILTE INODT UTURV SIITO
CDEEN MLSTN SNTLT AIIRH RHPCI NNHIK EAICO CVNTE OTSRD IPGNH ONOET
IIENP ITLPX ECHCE FOAOS

ZENDIA/JAAAJ-1 Engels (bericht # 091)

XYR DE OWN 4235KCS 230620T USM-99/00091

9516 8123 0605 7932 8423 5095 8444 6831

JAAAJ EUEBD OETDN GXAWR SUTEU EIWEN YUENN ODEUH RROMM EELGE AEGID
TESRR RASEB ENORS RNOMM EAYTU NEONT ESFRS NTCRO QCEET OCORE IITLP
OHSRG SSELY TCCSV SOTIU GNTIV EVOMN TMPAA CIRC ENREN OTSOI ENREI
EKEIO PFRNT CDOGE NYFPE TESNI EACEA ISTEM SOFEA TROSE EQOAO OSCER
HTTAA LUOUY LSAIE TSERR ESEPA PHVDN HNNTI IARTX LASLD URATT OPPL
AITMW OTIAS TNHIR DCOU NMFCA SREE USSDS DHOAH REEXI PROUT NTTHD
JAAAJ EUEBD

ZENDIA/JAAAJ-2 Engels (bericht # 244)

XYR DE OWN 6850KCS 231418T USM-99/00244

9536 8423 1345 8140 1871 5095 8444 4224

JAAAJ CTPIE NOEFR ERRDO AIVIO NEORS ENPIE OYCTD CARGD EPEIV ENOEE
ODEGI VIZZO VEROR GNTII NSONN SZFTI DOTCE VRENP EERDO AFAOE OMPFU
EHROL TMOHD MRSPO SWILF XEOHP RMYDL EADNE TWEPA AOTTE OHAOC CMCTI
MRXEI MYNTN LEABA AWUNY PYTWE ENLRC RDIEE JAAAJ CTPIE

ZENDIA/JAAAJ-3 Engels (bericht # 283)

XYR DE OWN 6850KCS 231613T USM-99/00283

9566 8723 1540 3749 6010 5095 8444 3915

JAAAJ ESTLG BREEI OALCP SNTET IEDNA FPEST VRTTI ODOFA BDNPS ESBHN
COREA ISNET EUENI ONAGK QLPOT ERAOU NNFIH EEIEO RVNAA OLSGO IMQOA
NUASO OGCOH RISDM TYONV UNTWO ETPNE OEMRI IALOE PPTLA RHIMI DPSFC
RTESM GTPUO NERVS ENGEN JAAAJ ESTLG

ZENDIA/JAAAJ-4 Engels (bericht # 317)

OWN DE XYR 5615KCS 231813T USM-99/00317

1026 5823 1700 9942 5445 8641 3872 6643

JAAAJ EHBED DASLT COIEO IERUR DMCST ATUII CTSTS HRTNT TSEER ESILS
MPHAE ANOSE TUREI TIURO QTROA AGTHE EIQEE EOADP EFTTN NRRNT HREEN
NASBU UDATN TROAF NBTCQ DIRT D EECID ASERN EDINN SQTEP PESOG OANRM
ENEDD IEOUU ENTHO CESOO ANESE MSORI EARER HTTEF PVELI OSANC ETFTE
TAURL TESSP LELOS LEIID TYRNE XNTEE AITAO RLCEO UIHSO ADETY TSOTR
NRAEF AHDCR DOAAM NSDUB GUTIT TASNS HSMSO ATDOP CNITM JAAAJ EHBED

ZENDIA/JAAAJ-5 Engels (bericht # 336)

VLH DE XYR 2310KCS 232106T USM-99/00336

6046 6223 2020 6530 1476 8641 7157 3323

JAAAJ TROHO LEAHN INHAI PMUMQ RRNNE DAOIE EERMH RIRIT ORBFR SOMOS
BAOMQ UUEAV TOUSN EDEAS TDUTR FWAEO ITEEN UOURN EYSBT KLETA RTBTP
EEOSD OITRT TJVEO MCZTU RNSSP OARMI LWEEI OSWEA XDPBT JAAAJ TROHO

Hoofdstuk 3

Monoalfabetische substitutie

3.1 PRACTICUM – Monoalfabeet oplossen

WERKSCHEMA

ADHRF SID QINVJX IH XDNAJIXJHAD VFH YINEVJ

.....

YDZEVJHJ PFO J TTDPJX J YE PDVEHJ JTTE

.....

DNAJ HFVWD DTTJ DN YIO QFHEAJ O NEYLJAEVJ

.....

DNLDXF WJVDX IHJ EYLDNEFH QIDHJ

.....

ABCDEFGHIJKLMNOPQRSTUVWXYZ

.....

Dit cryptogram is in het Spaans. Aanwijzingen uit de Spaanse taal:

- verdubbelde letter aan het begin van een woord is vrijwel zeker l, zoals in *llegar, llevar, llamar, lleno, lluvia, ...*
- 1-letter woord is y of a, een enkele keer o
- 2-letter woord beginnend met u vrijwel zeker un
- 3-letter woord eindigend op e meest que, soms fue
- 4-letter woord met patroon ABBC is meestal alli of ella

3.2 BONUS – Cryptogrammen met woordverdeling

Toelichting bij de navolgende series monoalfabetische substituties.

In de A-serie cryptogrammen is de woordverdeling van het cryptogram gegeven. In de P-serie zijn de woordscheiders weggelaten, maar ter wille van de leesbaarheid is het cryptogram verdeeld in groepen van vijf letters. In deze beide series is de taal Engels. In elk ervan neemt de moeilijkheidsgraad toe met het volgnummer. De cryptogrammen in enkele andere talen zijn ondergebracht in de X-serie.

Een woord in een cryptogram dat wordt voorafgegaan door een * duidt op een eigennaam. Bij sommige cryptogrammen is een woord gegeven dat in de klaartekst voorkomt; deze aanwijzing kan gecijferd zijn met het Caesar geheimschrift.

De *sleutelvariant* bepaalt het type van de sleutelconstructie. Deze wordt op de volgende wijze aangegeven:

- *K1-type*

Het klaartekstalfabet bevat de sleutel, het cijferalfabet is normaal:

```
pt: poultryabcdefghijklmnopqsvwxz  
ct: RSTUVWXYZABCDEFGHIJKLMNO PQ
```

- *K2-type*

Het klaartekstalfabet is normaal, het cijferalfabet bevat de sleutel:

```
pt: abcdefghijklmnopqrstuvwxyz  
ct: VWXZKEYBOARDCFGHIJLMNPQSTU
```

- *K3-type*

Beide alfabetten zijn gebaseerd op dezelfde sleutel:

```
pt: conquestabdfghijklmprvwxyz  
ct: HIJKLMPRVWXYZCONQUESTABDFG
```

- *K4-type*

Beide alfabetten zijn gebaseerd op een sleutel, maar elk op een andere:

```
pt: shoptalkbcdefgijmnqr uvwxyz  
ct: VWXYZJUPITERABCDEFGHIJKLMNOQS
```

Merk op dat het startpunt van het cijferalfabet t.o.v. het klaartekstalfabet kan variëren.

Het vinden van deze sleutels is niet nodig voor het inleveren van de oplossing. Echter, de sleutels van type K1 en K2 kunnen helpen bij het oplossen. De geïnteresseerde student wordt verwezen naar twee publikaties van William F. Friedman uit de Riverbank Series (de nrs. 15 en 21), die gaan over het reconstrueren van de sleutel uit een gepermuteerd alfabet.

MONO/A-1 Engels (sleutel is type K4)

"US WZY OQYS, PUA ZY SWQ ABOEQYS BT UEE UAZPUEY, YQVUGUSQC TGBP EUK
UAC IHYSZDQ WQ ZY SWQ KBGYS." *UGZYSBSEQ, *RGQQN VWZEBYBVWQG

MONO/A-2 Engels (sleutel is type K2)

ZOPR EVVB AMFG RXM JMWYAAYAW QVG KEOMP FJVOR RXM PVOGKM, HMARYVAYAW
FORXVGP, AMUPIFIMGP, HFWFSYAMP, PYWAP VG ZVBMP.

MONO/A-3 Engels (sleutel is type K1)

LBW SHMK FTCC LQIWV HS MGLKMLBV IWHIUW LWUU TKW: UCWV, ZTFGWZ UCWV,
VLTLCVLCYV TGZ OBTL OW TUU OKCLW CG HMK KWVMFWV.

MONO/A-4 Engels (sleutel is type K2)

EZV DFA NW ANYEZD JD DVGVEK=VJXZE. CFTV NW DVGVEK=VJXZE JD M QMC
TNMY WNCAFTM EZME OVYMTJLVD KNF WNC OCVOMKJYX.

MONO/A-5 Engels (sleutel is type K2)

GI TM TXBIMTHGRVTY NTATQRMX *NB. *TMWXBIFIM KBRGXF GERF RWXTY
FXMGXMX: TRBCYTMXF TBX GEX HYGRNTGX IZZ=BITW JXERVYXF.

MONO/A-6 Engels (sleutel is type K3)

KNS SNN QJIGS MRGQNK ONTZFS IK *I*J GIYDN, IKY DS VIQ SVN ERIGQ
ORCNGR FR CNTKY NTS SFIS FR BNTAY ADQSRK SN DS DK SFR ICSRGKNNK.

MONO/A-7 Engels (sleutel is type K2)

CT X BCOOBN AFGRBNIEN CM IXFENKGPM, RLKN CM OLN DXF RLG LXM MG
DPZL XM OG YN GPO GT IXFEN? *OLGDXM *LNFKV *LPSBNV

MONO/A-8 Engels (sleutel is type K3)

CX WJHBQWJHCMF OQ XQLQP VXEO OBJH OQ JPQ HJDVCXT JKEIH XEP OBQHBQP
OBJH OQ JPQ FJGCXT CF HPIQ. *KQPHPJXN *PIFFQDD

MONO/A-9 Engels (sleutel is type K2)

KF ODK JFTDKABCO ZFCD, W YFTTBKKDD JAFLNZ YFCJBJK FU CF TFID KAWC
KAIDD GDIJFCJ, KPF FU PAFT WID WXJDCK. *IFXDIK *YFGDNWCZ

MONO/A-10 Engels (sleutel is type K2)

IPC MUVEM KCYYVLQL GI MQG. COQ KGNNVQL G KGNTC CR NQL EGVOI, IUQ
CIUQN JYSQ EGVOI. IUQ KNQP ZQZJQNM PQNQ ZGNCCOQL.

MONO/A-11 Engels (sleutel is type K2)

CTOQFUCE DORT TATQFCYQYFL PL XTOFTS JOFTC ZGEF OE UFXTC FXTCDOA
EUGCQTE. XUJTHTC, COSYUQFYHT OEX YE MCUPATDOFYQ.

MONO/A-12 Engels (sleutel is type K2)

VYYCFZNBR IC IOS VBYNSBI *XVXQACBNVB YCZS CT *LNBR *OVWWJFVXN, V
WSFYOVBI YCJAZ XS DJI IC ZSVIO TCF ZNAJINBR XSSF.

MONO/A-13 Engels (sleutel is type K3)

UXXATYNRI CA *TAOUR MNBCATJ, GTNCNRI NR BMATCHMURY GUB NRFSRCSY WJ
*XNXSTA'B BSXTSCUTJ *CNTA CA ESSQ DQ GNCM MNB ATUCNARB.

MONO/A-14 Engels (sleutel is type K1)

HYS PORXBS CNHHN NW *PNYRRM *JSZGGCOBBSF, Q.A.Q. *HQFLQR: "VNR'H
BSH XN NW HYS IZRS!" RNH ISFM VNJR=HN=SQFHY, SY?

MONO/A-15 Engels (sleutel is type K2)

YILRK, RXEEMQK, ULIDMXF IRP ABXOW ILQ QFINE EQLOK STL KABXUUMQK
PQRTEXRU NBLKQ DTLPK XR NTOXN KELXWK.

MONO/A-16 Engels (sleutel is type K2)

*YGF *WGPYZF, JMFFUFN LJVXA EGJ *XVC, PVK LDZ EUJKL *VBZJUXVF LG
JMF LDZ BUCZ UF MFYZJ EGMJ BUFMLZK.

MONO/A-17 Engels (sleutel is type K1)

YBHHKZ EDZ TGGNUX PAZC WTN'OZ YZV XT YECW LZTLKZ VAEV ZOZUW CZP
LZUXTC WTN YZZV UZYBCHX WTN TS XTYZTCZ ZKXZ. *TDHZC *CEXA

MONO/A-18 Engels (sleutel is type K2)

XB YWI DLJ QTILJG XYNJ HMDNPSDFWB DZI SMPZVG FJSSJN YK XDZVPZI SMDZ
XB BYTSM JEJN IPI. *LJYNLJ *GDZSDBDZD

MONO/A-19 Engels (sleutel is type K2)

CPT EZM ZL EGP KPGC TSLGH ALGMT HL TEC, FIH AP TSLIXM HSUZW QLG
TLYP XPZRHS LQ HUYP FPQLGP TECUZR HSPY.

MONO/A-20 Engels (sleutel is type K4)

JFFCEW MZCPXPPEW, J.V.J. ZJWH XZ ACFG FQQV, CN XEZ OQNM ACFG XKCXK.
CM RFXAQZN CK *UEKQ=*UEFB JKG TJN J ATCMCNT OEFO.

MONO/A-21 Engels (sleutel is type K4)

PLOETPU ODFOHPJL OZVWOD EIVJBLY YDFLYXPL EJU CZEICXPL. AEZIPZ
ZPEODPL BFJBZXR FJYV YDFOHPY, ZPOETYWZPL NFXR AVNX.

MONO/A-22 Engels (sleutel is type K3)

FBERWBDP: "IMJ GVXQYAO SBUZ TVDFXER LCNWBP HCK" JICE X "FBQY DO NMK
JXZI UXHC SMLCE AXGVMW TVRP."

MONO/A-23 Engels (sleutel is type K4)

IKG OFTUI NMPT. IXBBCXGJ WUFZ IZXVCUI QMNHFGZ CXBFNQ PKNCUQ XG
IWFQMR VNMH OMDPFN EFNTUQ OS QUIUNZ IXQXGJ.

MONO/A-24 Engels (sleutel is type K3)

ZFI=ASFNCPB SWCFTK TI MPB SU MFNRFT ATEP VTCG RFIDS EGOICPX TN
EASVB ZKPFNPA TI *MPIDFKT PFCPAX.

MONO/A-25 Engels (sleutel is type K3)

SAUM ZUTLJY RPMCX BCDG. QCUM DRKWXI YPLU SAUM BPK BWK. DRJUXG BKPQ
AWXIA RWQQA POJKLGJSQJY ZCKS.

3.3 BONUS – Cryptogrammen zonder woordverdeling

MONO/P-1 Engels (sleutel is type K2, bevat woord: Caesar HYULYL)

VMAVU YOUAR OUFVW OQWRO MHEME FUFVM FEIFV FVHOV MAVUR MCWOL WRPWZ
ZMLAW FVPHZ RMVUU LRHOL MEEUE RFVUC HRXMP PMERU O

MONO/P-2 Engels (sleutel is type K2, bevat woord: Caesar JYLM IHM)

LDWJW VJWLD JWWGW JOFZK OEVGW JKFEK BOIWF EWT FN LDLQF COZZB WWSWV
EZLDJ WWT FN JWBFF AOESS FFZYB WFGVG GVK

MONO/P-3 Engels (sleutel is type K2, bevat woord: Caesar NBYLY)

QTXBA QWJUD LBCKT XHXQW JBDHX JFXZK PDHKT XUDLB CWBEB DQKTW KAWS
NEKTX HXAJB DHXJF XZKPD HKTXD NEASA JJXED LKZDS ABCWB ECDAB C

MONO/P-4 Engels (sleutel is type K2, bevat woord: Caesar MBUPYM)

ACLLA ZFBDO BWMLV TVSCB UQVXL YMHCB UVLZB RZVHE ZHCDY LIZVN ZHVUZ
VYMAL TVAZJ IVNZJ DQQVE EHDPC TVLZA RDBZE DMBYD QWZVH YUHDO LI

MONO/P-5 Engels (sleutel is type K3, bevat woord: Caesar LYQULX)

FPHMP TEOPX YVCTE OTPXH VCPQN EOPYZ OEXVP ZO CRV WEOPL OPWXH UWQYE
OPXWE OPCMX ZOZOC AWF XU VEXZP XQPHM PCOTT HCZHF ZPXPC MXZWF MHMXZ
OZOCE OIPEM LOOYZ OE

MONO/P-6 Engels (sleutel is type K2, bevat woord: Caesar NLONB)

HOXDU DWSFQ EEXII EOXET FEOUE HUIIV SDZSF DWKSF TXDXN UXBPD WPBES
FDWKS FTZTU XDWBN PTMEH PUD

MONO/P-7 Engels (sleutel is type K2, bevat woord: Caesar ZCMB-2)

IRETL RENKE MGXVR GVCRL RSRYA FCRSW OMHVR SFXTT AGGMC ALGXR VCRLR
SGMYA FCRSW OMHEH ASRKM SWXEY HTUHF ASXFF MBBME GHSAG O

MONO/P-8 Engels (sleutel is type K3, bevat woord: Caesar IHFS)

RJEDV URUIY DDWVQ URLSM EDGQV GWQYD QIVQM VGPLW TOYOQ RRWAG QIYDD
IMYKA ZYWVW DZLOR IMVGU PQVPR RCGYE RUARD Q

MONO/P-9 Engels (sleutel is type K2, bevat woord: Caesar QBYH)

CPSXO OCUJZ FJZEC IPBAG JMICI HJTFX OPPBQ MONXV ZBMCO PGXOG JMICI
HSBAI OPJNN XMNXV JQIHO XNNFA MOPMJ NAPBM JQHBP BARXZ XIPOP MAAPO

MONO/P-10 Engels (sleutel is type K4, bevat woord: Caesar WIQM)

BLFCD EAWEL IEPYP KDKWA ZBGZE EDHBZ ZMKNP EARJHKVKVE DBFRB SKJFY
ZMKMK DJYME ZDEAG JZMKP EDRJ

MONO/P-11 Engels (sleutel is type K4, bevat woord: Caesar QBI)

GJKEB XMKWN NWUBK FMLKL ZWUGA NQLPD QWLAX BLAFD PJUAF DPUSN KFDUB
ECBEE LDZLC FEVLE JBGLV

MONO/P-12 Engels (sleutel is type K3, bevat woord: Caesar VON)

YGGDR TIPIT NYUGR KIRZC IPYTM XCUWX VYZVW XZCXH WZDRT AXCXO IHOWN
RTVXW XTHOW HWTYG TCWWH CAWOO ITRSI ZVIRZ XCWHR Y

3.4 BONUS – Cryptogrammen in andere taal dan Engels

MONO/X-1 Nederlands

BFOILLHAHXGH BFOYUPAHX BFOHUGHX BFOYYUDHU BFOPHUPQT.
BFOCLHAUCFOHXG BFOYYL BFOUHWPHUPMH BFOYYUWHHBLHA LYH. BFOYYAJYHLHXG
BFOIPJHXG BFOYYUUYTCCU PX.

MONO/X-2 Nederlands

BIEUSCYW BIEYRWEFYCSECZS BIEURW BIEMRASNSRQS BIEUUAZSBMPXYWS
BIEYRWIMMEQSRBXUHB. BIESFAEYZAS BIESSABCMNDSSBCSE BIEMASNUUB.

MONO/X-3 Duits (sleutel is type K2, bevat woord: kommt)

HVC QRHLL EHVCM QYL LFBB RL ZRORNRE, OYLL HVC LF MKYNKHI ZHE. RHE
DYRKVCRE YNL YBMRE XRHMR, OYLL AFDDM DHK EHVCM YNL ORD LHEE.

MONO/X-4 Duits (sleutel is type K2, hint: OEBC = fpvw)

ZSKQR JXGAA CSAAMZ, AGZLMWZ ITKQ OTMW LSM ZIKQCMXR RTZ, CIA LSM
BGWCMXR OTMW TZA PMRIZ QIR, QMSAAR MSZ YMAKQZ AMSZ.

MONO/X-5 Duits (sleutel is type K2, bevat woord: mogelijk)

OI PUDFUS JYRUT YI EOSR RUC DQXOFFUS ITUWEYQX YDF XOUSWUSRU DFOXE
RCOXF RCUYDDYUW QI EOSW (OED UYSU XTCS VHUC DUOSQUD.)

MONO/X-6 Duits (sleutel is Engels, type K2, bevat woord: grosse)

XBEFFV YQHFOQGMV PQXG VZCV NQHF ZN UQHR IVBFGVSOG, DUEVGMUZY NQSYG
FZV VZCVC WUZVXVCTVC FDBHCX QHW ZYBV HCXUHVSOUSYV RVHGV.

MONO/X-7 Frans (sleutel is type K2, bevat woord: paysans)

SY UDKGCTSQHJY BTGWATQJ, HTW TK XDH, HKG SYH WAYBQCH XY BDCJTMCY,
TLYW XYH WDSSYMKYH, TLYW XYH BYXYWQCH, TLYW XYH BQSQTJCJH ETPHTCH.

MONO/X-8 Frans (sleutel is type K2, bevat woord: humaine)

PU BVCBPA LWVAPA DVCSVXT, L'PAB JCAAX UP EJA DVCSVXT. PB JLLPEBPT
MPA APTDXBCMPA PB MPA SXOXBPA, AJUA NCVX XS U'H J EJA M'JLBXVU
WCOJXUP.

MONO/X-9 Frans (sleutel is type K2, bevat woord: que-2)

XI VBUETKO Z'OUÉ VIYITU UT JOXXO NBO UMBU BZ LORBTUOYOZE, NBIZL
OXXO AMQEO ZMZ AIU BZ JIZLOIB YITU BZ YIUNBO OE AOQUMZZO ZO UITE
NBO K'OUÉ.

MONO/X-10 Frans (sleutel is type K2, bevat woord: les-4, QTEN = bjkz)

UX VXSGDX XRRPZPFOSX WXF OSYADRPGOASF FHD UXF PHGAF IAUXXF, UXF
RAGXHDF, UXF BOXVXF XG UXF BUPCHXF W'ORRPGDOVHUPGOAS.

MONO/X-11 ???? (sleutel is type K2)

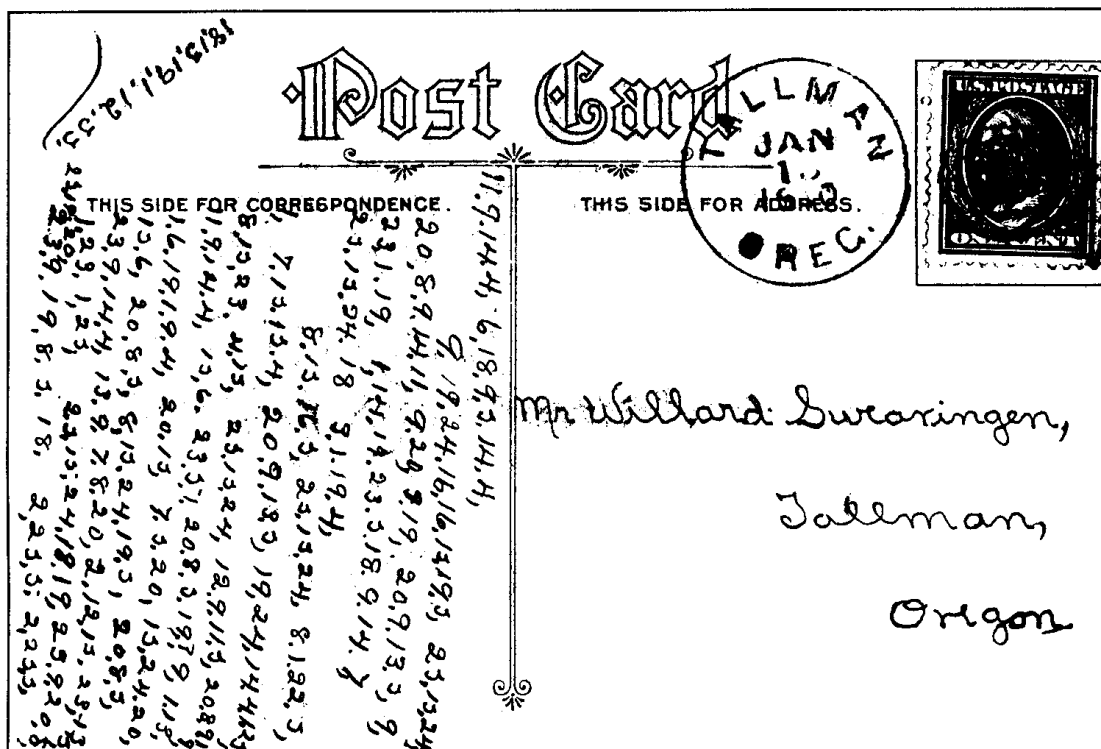
GVONXL JQNKX ANK VG UTGJQIQZ JK TKOGVGT VG TZLG YG XKQDKT JK VG
MQTG JVKL KXGWZTGUL ANK LK IKVKHTGYG G *HGTIKVZXG.

MONO/X-12 ???? (sleutel is type K2)

ANEB CMSQNAANAB BNEGTA M PTEJ IEX ANEB TAAEXTAD, RMXB ANEB AT
CNEGNAB CMSQNAATS M PTEJ IET ANEB TAAEKNAB. *FM *SNPWTUNEPMEFD

MONO/X-13 Frans (sleutel is type K2, bevat: contre les

VRRVV FGZIA HZFFP BGVSL BGDVR VFUVJ PFGPG ZLBFS PHFVV FAPDS VFGVD
DZQRV FWRVP HMIPZ FRPTH FGZSV DVRZX ZVHFV ALFFV UVRVF ILNVB F



Onderschepte ansichtkaart uit 1910, Engelse tekst

Hoofdstuk 4

Polyalfabetische substitutie

4.1 PRACTICUM – Porta oplossen

PRACTICUM-1 Engels (woord: collision, lange sleutel)

MPHSY XBLAM IZXJK GXKJD WNRQM MGSIR GAKFH MYGVH ETIEX NQXDE AXMDR
KGRXU AYEYX QMSNO EXIMQ SEIWR FGWJR XKDPT EELPA GCWOJ

Dit cryptogram is een in het Engels gesteld marinebericht in het Porta-systeem en het bevat het waarschijnlijke woord COLLISION.

Hanteer de hierna beschreven werkwijze voor het oplossen van dit cryptogram:

1. Bepaal de plaats van het waarschijnlijke woord op basis van het substitutiepatroon en reconstrueer daarmee een (klein) deel van de cryptogramsleutel.
2. In onderstaand schema moet daartoe op de bovenste rij puntjes een 1 worden ingevuld voor cryptogramletters A–M en een 2 voor N–Z. Voltooi dit eerst.
3. Het waarschijnlijke woord COLLISION heeft het patroon 121112122, maar dat zal zo niet in het cryptogram terecht komen. Bedenk dus wat het patroon wordt na vercijfering en lokaliseer het in de reeks van 1'en en 2'en.
4. Daar waar het patroon matcht, kan met behulp van de Porta-tabel (achter in dit werkboek of het exemplaar in de syllabus) de bijbehorende sleutel worden bepaald. De sleutelletters in de Porta-tabel zijn de letters vooraan de regel waarin cijfer- en klaartekstletter onder elkaar staan. Ziet men bijvoorbeeld dat een letter X in het cryptogram in de klaartekst een F is, dan moet de bijbehorende sleutelrij die met sleutel KL zijn, want in die rij staan de F en de X boven elkaar.
5. De twee sleutelletters kunnen worden genoteerd op de tweede en derde rij puntjes. De onderste rij in het werkschema is voor de ontcijferde tekst. Probeer een (stukje) van de (Engelse) sleutel te vinden. Let op: in het Porta systeem heeft men steeds de keuze tussen twee letters. Dus als de sleutel het woord MARINE zou zijn, dan vindt men de volgende twee reeksen waaruit de juiste letters moeten worden genomen:

M	A	Q	I	M	E	→	M	A	I	E
N	B	R	J	N	F			R	N	

6. Het oplossen kan nu op verschillende manieren verder gaan. Probeer bijvoorbeeld naar rechts de sleutel aan te vullen. Ontcijfer hiermee en kijk of het begin van het woord dat na COLLISION komt kan worden herkend en aangevuld. Kan het woord worden afgemaakt dan komen daarmee nieuwe klaartekstletters beschikbaar om de sleutel mee uit te breiden. Hetzelfde kan gebeuren door naar links te gaan. Op een gegeven moment zal de sleutel zich herhalen en kan het gehele bericht worden ontcijferd.

7. Een tweede mogelijkheid is om te bedenken welke woorden op COLLISION zouden kunnen volgen of er aan voorafgaan. Met een hit kan dan de sleutel worden aangevuld.
8. Als dit allemaal niet helpt, moet gebruik gemaakt worden van het feit dat de sleutel periodiek is. Neem het gevonden deel van de sleutel en begin te ontcijferen in de veronderstelling dat deze op positie 1 in het cryptogram start. Meestal valt na het ontcijferen van twee of drie letters al te zien of deze sleutelpositie iets gaat opleveren. Als geen goede ontcijfering resulteert, verschuif de sleutel dan naar positie 2 en herhaal het proces. Doe dit net zo lang totdat ontcijfering goede (delen van) woorden oplevert. Begin dan met proberen op positie 11 dat voorkomt wellicht enige frustratie. Echte cryptoanalisten hebben daar natuurlijk geen last van ;-)
9. Zodra een goede positie voor het gevonden sleutelfragment is gevonden kan een schatting worden gemaakt van de lengte van de sleutel. Tussen de hier gevonden sleutelpositie en die van het woord COLLISION zullen immers een geheel aantal herhalingen van de sleutel liggen. Daarmee kunnen andere posities in het cryptogram worden ontcijferd en dan ontstaat genoeg klaartekst om de ontcijfering af te kunnen maken.
10. Het werkschema is zo ingericht dat op de eerste regel met puntjes het patroon van de cijfertekst moet worden geplaatst. De ontcijferde klaartekst komt op de regel daaronder. Gebruik de regels k1 en k2 voor respectievelijk de eerste en de tweede letter van de Porta-sleutel. Zet op de onderste regel een letter uit òf k1 òf k2, zodanig dat een begrijpelijke sleutel kan worden gelezen.

WERKSCHEMA

ct: MPHSY XBLAM IZXJK GXKJD WNRQM

12122

pt:

k1:

k2:

kk:

ct: MGSIR GAKFH MYGVH ETIEX NQXDE

.

pt:

k1:

k2:

kk:

ct: AXMDR KGRXU AYEYX QMSNO EXIMQ

.

pt:

k1:

k2:

kk:

ct: SEIWR FGWJR XKDPT EELPA GCWOJ

.

pt:

k1:

k2:

kk:

4.2 PRACTICUM – Beaufort oplossen

In de volgende opgave moet een Beaufort worden opgelost met behulp van een *crib*. Dat is een stukje klaartekst waarvan men weet of vermoedt dat het in het cryptogram voorkomt.

PRACTICUM-2 Engels (woord: ammunition; zie werkschema)

MDSTJ LQCXC KZASA NHYLN M

WERKSCHEMA

01: MDSTJLQCXC ammunition s: MPENWTJKLP	02: DSTJLQCXCK ammunition s:	03: STJLQCXCKZ ammunition s:
04: TJLQCXCKZA ammunition s:	05: JLQCXCKZAS ammunition s:	06: LQCXCKZASA ammunition s:
07: QCXCKZASAN ammunition s:	08: CXCKZASANH ammunition s:	09: XCKZASANH ammunition s:
10: CKZASANH ammunition s:	11: KZASANH ammunition s:	12: ZASANH ammunition s:
M D S T J L Q C X C K Z A S A N H Y L N M		
s:		
pt:		

We veronderstellen dat het cryptogram een (Engels) sleutelwoord heeft. De positie van de crib wordt gezocht door deze overal te plaatsen en de bijbehorende sleutelletters op te zoeken in de Beaufort tabel. Wanneer de crib op de goede plaats staat, wordt (een deel) van de sleutel leesbaar. Om de periode van het cryptogram te bepalen wordt met de gevonden sleutel op andere posities ontcijferd, net zolang tot ook daar goede klaar-

tekst verschijnt. Daarna moet de rest van het cryptogram worden opgelost en zonodig de overige letters van de sleutel worden bepaald.

4.3 BONUS – Porta normaal alfabet

PORTA-1 Engels (woorden: cargo, ships, convoy)

VNVHX ZRILC FDNZX EQLZE IVGCJ EFNMB CTVRC

PORTA-2 Engels (woorden: cruiser, destroyer)

GFDBL VEWLD EOFRW EZLSN DXNJL CAKZK

PORTA-3 Engels

FGEUZ KXTVK HUWMO JGIFY XTPDS NEQMH BFYLR OOHCP ZLUPD LPDRJ CPARZ
YDGJL JRDJV MZWQC QSZPO CGBEN MKKPV TGPLP IPSTZ CLROI SMPJY FARNK
EUZDM RAOPE NTIDB NNMHR FDJZW UYDAG BEUMF KEUZQ DGAOW PCZCA NDKPG
RDFMF FFIEU GEVPA VTFAQ SPGWF GDJQD WFWYP NLKDX YZWKT QQVUV QLSEN
FTLNH WSLRB CXFZW MTVFQ CEWMP LTLXT ESIYR RFDNL VWLQR ZKVES WMPPL
YGVFC HLGPU ANDKH UNTOX RRUPV ULSMN EKUNS GBRRE GYCVG TMAFQ YLVOX
EBTSA NLLGM SWMYS NKXEJ AJPIN UUCVQ WGANL BMYFF KARYL QBOKL XALXT
TGUZM SHQEG WFGUW ZKMEF QWMNK DMSER WXYDC PAYWS PEOUO RDYOP ALFTF
ENSXA LXTGO AHUNL EVNMZ TPPPY LRULG LRYQL QRWTP TZTEU SKAVM

PORTA-4 Engels

UWJTN ULFWV LVFLC COOTL RLWRF ILEND CQJQV ZVTBQ ZKPRP TBYWE KFLQP
ZIRFR XPCQW KLEFL TTNRU NESRX WJLRZ PRUPW THVXK IVGTN EEYBK QZBJN
LFNPQ BEAAF

4.4 BONUS – Vigenère normaal alfabet

VIGENERE-1 Engels

AUKHY JAMKI ZYMWM JMIGX NFMLX ETIMI ZHBHR AYMZM ILVME JKUTG DPVXK
QUKHQ LHVRM JAZNG GZVXE NLUFM PZJNV CHUAS HKQGK IPLWP AJZXI GUMTV
DPTEJ ECMYS QYBAV ALAHY POEXW PVNYE EYXEE UDPXR BVZVI ZIIVO SPTEG
KUBBR QLLXP WFQGK NLLLE PTIKW DJZXI GOIOI ZLAMV KFMWF NPLZI OVVFH
ZKTXG NLMDF AAEXI JLUFM PZJNV CAIGI UAWPR NVIWE JKZAS ZLAFM HS

VIGENERE-2 Engels (woord: vertical)

AIEVI RLXRY TERRB MTWWF ZZYOC RSCFB CQLZG LWFMD YOZXA BXOCU ZBCPH
 MGZKH CTREF EQBQS RESOE ZEUQN VPGFX FZZYH UOXMH HFINU FPVIR ZKOCR
 TWGCG CFMEZ EAO CY MLLCU AENSY YAGLL BWEFC Z

VIGENERE-3 Engels (periode = 8)

HBXYE QKPOF ZCOQE BKULZ NAFDH BXMLK FBWYL EBWKR ZYZCO QEBGC GEHAI
 CJIEF TEFLA UMNHA UGBUM COYZR MUGOV EFJSH VPOJC WPSMS EIFFO QDGAH
 CCM

VIGENERE-4 Engels (een Gronsfield)

XUHUW LRLWV URWPL RLUWZ CITLN IQWBN UBVKN UNKJK ICQXU TQVOI LAIMA
 JQMHU BMWBR VOBWQ MJSUP QBBQL HZMJB NZUPQ WLAHO KMCWU PGM

VIGENERE-5 Engels (een Gronsfield)

YLFZR LCUKV WTUGC WNKXM BIPPR SJALV QPQVS WRYNX KLHIS ICQJC FTHEU
 HOVZZ EICUB IJNUV GKJDF QOFGF JTJIV ETWXM YPKYP LCLIA ZEVHB

VIGENERE-6 Engels (periode = 10)

IPUSR UKUUY WTJIE BOFHM WYGKY ACZCS IAVLI JEYSB WSSVG FPHIY AFWXS
 RKSTW WZASL TQZWS KRFXR RNNFJ MPWMN JGHFH PBXXH VHHPQ MQYSL UGUTQ
 MRUIA XGUSW IGASN SGMCW MGZIT IQQOS ENJ

VIGENERE-7 Duits (woord: -auf, periode = 8)

WRXBY EGMAM LLPNM TIQXK EAAOK KZMPM YNJGA XQIHY QVGZ SYXKG DXYUH
 IHENY DCBZA RXBYJ OSCIK FLNHM ERMXC IBRSS EEEEC MJYXU PRBTH IGYTE
 FIWRG TMELE QVNXN KOSZO XNNHN JVYOB PLYPH EFHET YSZEK TFFGJ ERVAP
 FHJER SNGIY QXENV S

4.5 BONUS – Beaufort normaal alfabet

BEAUFORT-1 Engels (woord: greenville)

ODPHN VVMCE WEA VP MG VAC EPVIR KRNRE KZSRW TRRGR JZOYE NVDSI RRITJ
 XHYUR EMGVC

BEAUFORT-2 Engels (woord: regiment)

PGSGG DNRUH VMBGR YOUUC WMSGL VTQDO

BEAUFORT-3 Engels (MJYYWB)NFNIE YLBHT UUUBB UECXW SSRTU UYKUJ FIEQZ YQEW BAQQN GHWEL YJXDQ
XBDAE IDOMT TICTB RCNHG QBDQ**BEAUFORT-4 Engels (ZUCNB-2)**GAJZQ MUIAM EUABA NDLAW WMPHU TAZSU NBAUQ BJRJM IAPDW YXRPP ZCAEA
AJFFF GJNOK JVIBY ZKEBY CQAUQ BJLCS RTNDS GWPRU IH

4.6 BONUS – Vigenère met gemengd alfabet

Gewoonlijk is de beste oplosstrategie om eerst de periode te bepalen. Dat kan door het spotten van herhalingen of door het uitrekenen van de Index of Coincidence voor periode een reeks waarden voor de periode (zie het hoofdstuk over cryptanalyse in de syllabus).

In de berichten MIXEDKLAAR is het klaaralfabet gemengd en het cijferalfabet is normaal. Oplossing van de polyalfabetische substitutie geeft als resultaat een monoalfabetische substitutie die ook moet worden opgelost.

MIXEDKLAAR-1 Engels

QEOVK LRMLZ JVG TG NDLVK EVNTY ERMUE VRZMO YAAMP DKEIJ SFMYO YHMME
GQAMB UQAXR HUFBU KQYMU NELVT KQILE KZBUE ULIBK NDAXB XUDGL LADVK
POAYO DKKYK LADHY BVNFV UEEME FFMTE GVWBY TVDZL SPBHB XVAZC UDYUE
LKMMA EUDDK NCFSH HSAHY TMGUJ HQXPP DKOUE XUQVB FVWBX NXALB TCDLM
IVAAA NSZIL OVWVP YAGZL SHMME GQDHO YHIVP NCRRE XKDQZ GKNCG NQGUY
JIWYY TMAHW XRLBL OADLG NQGUY JUUGB JHRVX ERFLE GWGUO XEDTP DKEIZ
VXNWA FAANE MKGHB SSNLO KJCBZ TGGLO PKMBX HGERY TMWLZ NQCYT TMWIP
DKATE FLNUJ NDTVX JRZTL OPAHC DFZYY DEYCL GPGTY TECXB HQEBR KVWMU
NINGJ IQDLP JKATE GUWBR HUQWM VRQBW YRFBF KMWMB TMULZ LAAHY JGDVK
LKRRE XKNAO NDSBX XCGZA HDGTL VKMBW ISAUE FDNWP NLZIJ SRQZL AVNHL
GVWVK FIGHP GECZU KQAP

MIXEDKLAAR-2 Duits

UTEWO YLTOA RNLT Y IROVO VZPDX FDQFW GZSER NJKQL NJUOT WEKEE YPDHP
 PYPEH JKQLN JUIRA JPAEO PMPPB QCQBO TOLGS ABTUZ ZYEEA XJPCQ LXQEE
 ABXJL OOABP AJETD SKOHL VZTSD FUXLT NBFZP UJWTH LEFPE LQRB J PSRFE
 BPJAX OKEPP XQBCB AUYYK ZPXOL RSMXO AKBSS OVPJA GHLBE LOJGT HTZOV
 PNNDT WVZPZ VZUZQ XQVOH VPOVB PPUOL ZGOUN BRDXY OLIK PYLKJ PXHKX
 ZZBEL JPIYO LIZUP DEPOK WRPUX JIBWZ YQPDR PJYXY WIYNJ YWCZV SSWTY
 SSBYV CQOVZ ZAMPM PDL PZ OFZNC RMGQJ XJOAO ZQNTZ RFLEF PELQ

MIXEDKLAAR-3 Duits

UQOXW TOBMO XWWPA NUUNV OXGXU UOZGA XWOF S AWODK VUMQL NTUME ZUSAL
 XMFLT EBROS AGPSH YFUBM NVSGP OQXEX QKOSQ LBQXL UFUVG SSXSO GUCRQ
 ZMQTM QDNUM UWVHQ WGQOH RKGHS XSSPP USIUT AMYSS CENYY DLHUS STMQQ
 MYDXW NMJWQ HMSQK GHZQS AKVSQ ISXTP HYQXB MLCUM HSQDU QGLIS WQURE
 CUXQK SRAPQ KXSLM SKHUK XNRJX AFBKH TUZEM SYFFY XHYDF QSJIU JHSEI
 ZMGRN PWRVT HYNFO VFSTX WVRJU MAIGT MGOQV QUMNA UFZLW CFJXJ QSOST
 MVXHB SGPCM JWGWW KJADG DNUSG SUSLU EQRFI TKUMF RUTHO JIUIE QPDKU
 XMNBU IAMYS SMPMQ WUHQ S QXWIJ MNRVN ORYAF NVKHU VGORH ILMZE VQSLG
 LNBUE XRJIT UWDHZ SFRTL RUNTD NPK

In de berichten MIXEDCIJFER is het klaaralfabet normaal en het cijferalfabet gemengd. Hier moet voor elke sleutelletter de alfabetpermutatie worden bepaald, bijvoorbeeld door *symmetrie in positie* toe te passen of door gebruik te maken van *isomorfen* (als die er zijn). De opgaven zonder aanwijzing zijn bedoeld voor de betere doorzetter.

MIXEDCIJFER-1 Engels (symmetrie in positie, woorden: aboutonethirdofapoundof)

WFRFO XBUPD HMONH GBJJF MTRAP MJXMN HCBDI TRNUH OJXNR FCQAJ FBHPV
 APZWJ RXAAQ UYTNS AAQCN CBGKT JKFNU YVSND VIKGS IUIJF MTUAY DIKWE
 DHOCX HFATY JINSO

MIXEDCIJFER-2 Engels

QWBRI VWYCA ISPJL RBZEY QWYEU LMWGW ICJCI MTZEI MIBKN QWBRI VWYIG
 BWNBQ QCGQH IWJKA GEGXN IDMRU VEZYG QIGVN CTGYO BPDBL VCGXG BKZZG
 IVXCU NTZAO BWFEQ QLFCO MTYZT CCBYQ OPDKA GDGIG VPWMR QIIEW ICGXG
 BLGQQ VBGRS MYYJY QVFWY RWNFL GXNFW MCJKX IDDRU OPJQQ ZRHCN VWDYQ
 RDGDG BXDBN PXFPU YXNFG MPJEL SANCD SEZZG IBEYU KDHCA MBJJF KILCJ
 MFDZT CTJRD MIYZQ ACJRR SBGZN QYAHQ VEDCQ LXNCL LVVCS QWBII IVJRN
 WNBRI VPJEL TAGDN IRGQP ATYEW CBYZT EVGQU VPYHL LRZNQ XINBA IKWJQ
 RDZYF KWFZL GWFJQ QWJYQ IBWRX

MIXEDCIJFER-3 Duits

BHMTQ TLENN OWPRZ UBQXB OKBQP TKTMT CCERE OCRKE RHJNQ LQIZR HFQXN
 KVZJZ ZRRNI SUFQT BTZRA GRSIB TFWOZ CQIYX JSUFQ EUQPN QLPQA YXPCL
 MZBTZ FYNBQ XBOKB SYMMJ BWJKZ MQTIB ATWNM QHNXO UKNXB HPKSM QVIZE
 DJOHH HIBTI AQYRY OHHYE GNKIF VOMRN GVZZT AVBSJ TVUQO ZZHEYX ZLFQT
 ESMEQ TMIPQ PFBTZ RAQNR PQRNO WTLQB GCINQ GHOTQ YLNRH HVTTI ZFNIY
 SKHQT ETRUM JETPR QYCIH TKTEO HWVXE LCBMJ BYOVA XFOHS UQHQP KPNWC
 PBMLF OTMEV XCLEE QETRH TFDIZ CQTTY OEVTF OCBOK XOIWQ XEOZM EGECH
 RQYHY OHHFQ GXRKE WKTQQ BLOZC QYIOU RSLBW OBQTB MNKXZ

MIXEDCIJFER-4 Duits

GSXVH CBRNO ACTST WBEPP OSUZI PJKCK YLICB HWBYI VZSOY WPJCQ DLNMH
 DNVYB CASFN JOPQK TTLRZ CJSSZ VCTBV UUBHR VSIAR HRCMK LFUPY ZSBAH
 EZEFX VXCCQ DLWZC CSNVZ XIZAN CAPZO UTOVC CBBYC PWCNS QOAWR YXNJL
 IEDSN BQPPU XXCZK CPCNN YPPQS BEBPQ KTOBS LNQTF LRCMZ EHSIJ CBZVQ
 RCSZS QOAWR YTOWR HCLLV ZAXZZ SIZIZ EKBUX VMJVMKZNYK ZVKCP TCZSV
 BSYGZ SYDIO CBHWB YIVZS OKECC BVNJR CZLXP BWPPQ SBBWL NLOWK TNCSN
 CVIUQ LEPNZ ICBTT KLIYB ODJBZ IKAFL EPFVM KELPN NXHSW ZSCTX DITZB
 RNBRZ UDNTV RICSX OZWZI ZAFKP TRQTT YRZLO SJLQJ QEDUK NMHDN VARIZ
 BGNJQ PJFDO L

4.7 BONUS – Isologe cryptogrammen

De nu volgende opgaven zijn gebaseerd op het verschijnsel van de zogenaamde *isologe* berichten. Een isolog noemt men een bericht dat op twee verschillende manieren is gecijferd. De cryptoanalist heeft aldus de beschikking over twee cryptogrammen en weet (of vermoedt) dat de inhoud van beide dezelfde is. Hiervan kan in veel gevallen gebruik gemaakt worden om het bericht op te lossen.

Het bericht in kwestie is van origine een enigma bericht van 21 mei 1940. Het werd door een Duitse eenheid verzonden ten tijde van hun opmars richting Duinkerken. Voor deze opgave is het opnieuw gecijferd met het Vigenère systeem, klaar alfabet normaal, cijfer alfabet gemengd. In het eerste cryptogram is de sleutellengte 3, in het tweede is dit 5.

Bepaal het gemengde alfabet door *chaining* gevolgd door het opzoeken van de juiste decimatie. Het cijferalfabet is hier het gemengde alfabet. Dit betekent dat vóór de laatste ontcijferstap eerst een substitutie moet worden uitgevoerd, het resultaat daarvan is dan een gewone Vigenère.

Voorbeeld. Stel dat de beide alfabetten luiden:

HYDRAULICBEFGJKMNOPQSTVWXZ (cijfer alfabet)

ABCDEFGHIJKLMNQRSTUUVWXYZ (klaar alfabet)

dan geschiedt reductie van het cryptogram tot een gewone Vigenère als volgt:

DOSJY... (cryptogram)

CRINB... (reductie)

Aanwijzing Na de reductie is oplossing van de Vigenère met periode 3 natuurlijk het eenvoudigst. Gebruikt men hiervoor de methode van het nalopen van de generatrix, dan blijkt het goede antwoord pas als men in elke generatrix *alle* gelijkvercijferde letters van het cryptogram meeneemt. Volstaan met bv. slechts een tiental letters leidt gemakkelijk tot een valse oplossing. Na het bepalen van de oplossing moeten nog de sleutelwoorden van de beide cryptogrammen worden gevonden.

Dit probleem is niet eenvoudig, maar met in acht nemen van de nodige zorgvuldigheid is de analyse zeker te doen.

ISOLOG-1 Duits

periode 3:

DOSJY ZGYBF ZYAYT KBOKF NUDQP YDTFE AILPY EADTC OZLHE ZNAZM EPWUF
OFNWN SUVZM CYLPO VAABA NDRZN AW

periode 5:

IYWUL VEVIR OPKVE NPSVE IREUC NYGXP GTCZL FYEXX GQMBP AXBIQ FMTYR
GRXTY UEZIQ LVZTB JSKLM PRVIR XT

Hieronder volgen nog twee van dit soort paren cryptogrammen, beide alfabetten kunnen gemengd zijn. De eerste van de twee opgaven heeft nogal korte cryptogrammen, waardoor er niet genoeg betrouwbare herhalingen in zitten om de periode mee te bepalen. Gelukkig is gegeven dat in beide cryptogrammen de sleutel dezelfde lengte heeft. Dankzij dit feit kunnen ook zogenaamde *verticale* herhalingen benut worden. Dit zijn posities zoals de 4e en de 44e letter; in beide is de letter in het eerste cryptogram een E en die in het tweede een L. Dit herhaalde verticale digram EL duidt ook op de periodiciteit van de sleutel. Het tweede paar cryptogrammen toont wel enkele herhalingen.

ISOLOG-2 Engels

YHYEX UBUKA PVLLT ABUVV DYSAB PCQTU NGKFA ZEFIZ BDJEZ ALVID TROQS
UHAFK

CGSLZ QUBMN CTYBV HLQFT FLRHL MTAIQ ZWMDQ NSDWN LCBLQ NETOC VSNZR
BJNOQ

ISOLOG-3 Engels

VMYZG EAUNT PKFAY JIZMB UMYKB VFIVV SE0AF SKXKR YWCAC ZORDO ZRDEF
BLKFE SMKSF AFEKV QURCM YZVOX VABTA YYUOA YTDKF ENWNT DBQKU LAJLZ
IOUMA BOAFS KXQPU YMJPW QTDBT OSIYS MIYKU ROGMW CTMZZ VMVAJ

ZGAMW IOMOA CODHA CLRLP MOQOJ EMOQU DHXBY UQMGA UVGLQ DBSPU OABIR
PWXYM OGGFT MRHVF GWKNI VAUPF ABRVI LAQEM ZDJXY MEDDY BOSVM PNLGX
XDYDO PXBYU QMNKY FLUYY GVPVR DNCZE KJQOR WJXRV GDKDS XCEEC

Hoofdstuk 5

PRACTICUM – Oververcijfering oplossen

5.1 Slag by Midway

In het voorjaar van 1942 stoomde een Japanse invasievloot op naar het eiland Midway. Men zal zich herinneren dat in december van het voorafgaande jaar de keizerlijke marine met groot succes een onverhoedse aanval had gedaan op Pearl Harbor, de Amerikaanse vlootbasis op het eiland Hawaii. Bij die aanval was een aanzienlijk deel van de Amerikaanse vloot in de Stille Oceaan vernietigd, waaronder enkele grote slagschepen. De Amerikaanse vliegdekschepen waren ten tijde van de aanval echter buitengaats en bleven zo gespaard.

Nu was de Japanse marine – onder opperbevel van admiraal Yamamoto – bezig om de buitenste verdedigingslinie van het keizerrijk naar een punt ver van het vaderland te verleggen, ja zelfs een directe bedreiging te gaan vormen voor de Amerikaanse westkust. De uitkomst van de zeeslag, die in de buurt van het eiland Midway werd uitgevochten, zou daarvoor van beslissende betekenis blijken.

Het was in zekere zin een merkwaardige zeeslag, omdat de elkaar bevechtende vloten in het geheel niet in elkaars directe nabijheid zijn gekomen. Dat was kort daarvoor ook al eerder gebeurd bij de slag in de Koraalzee. De slag werd uitgevochten door middel van vliegtuigen, die elkaars schepen bombardeerden en met torpedo's bestookten. De sleutelrol in deze slag was daarom weggelegd voor de vliegdekschepen aan beide zijden.

Omdat de Japanners niet wisten waar de Amerikaanse vliegdekschepen zich bevonden (hier bij Midway of elders in de Stille Oceaan) hebben zij luchtverkenner uitgestuurd om naar ze te zoeken in de directe omgeving van Midway. Hoe belangrijk dit was, bleek tijdens de slag. De Japanse admiraal moest op een gegeven moment kiezen tussen twee alternatieven: (1) het uitrusten van zijn vliegtuigen met bommenrekken voor het bestoken van de verdediging op Midway, en (2) het monteren van torpedo's tegen de Amerikaanse vliegdekschepen. In de veronderstelling dat de vliegdekschepen te ver weg waren om een bedreiging te vormen koos hij voor het eerste. Dat bleek de verkeerde keuze. De ruïne die na de slag van zijn schepen overbleef, was het directe gevolg van het te laat signaleren van de Amerikaanse vliegdekschepen. In de berichten die we in deze opgave decoderen zullen deze elementen van de slag bij Midway voorkomen.

5.2 Systeem van vercijfering

Het systeem van vercijfering werkt als volgt: Eerst wordt met behulp van een 10×10 vierkant de boodschap vercijferd tot groepen van 2 cijfers (*dinomes*). Vooraan komt de rij-coördinaat, daarachter die van de kolom. Bij het resultaat van deze eerste vercijfering wordt een periodieke reeks optelgetallen geteld (modulo 10 optelling).

Codeertabel										
	1	2	3	4	5	6	7	8	9	0
1	A	1	AL	AN	AND	AR	ARE	AS	AT	ATE
2	ATI	B	2	BE	C	3	CA	CE	CO	COM
3	D	4	DA	DE	E	5	EA	ED	EN	ENT
4	ER	ERE	ERS	ES	EST	F	6	G	7	H
5	8	HAS	HE	I	9	IN	ING	ION	IS	IT
6	IVE	J	O	K	L	LA	LE	M	ME	N
7	ND	NE	NT	O	OF	ON	OR	OU	P	Q
8	R	RA	RE	RED	RES	RI	RO	S	SE	SH
9	ST	STO	T	TE	TED	TER	TH	THE	THI	THR
0	TI	TO	U	V	VE	W	WE	X	Y	Z

Als voorbeeld wordt de tekst HIGASHI NO KAZE AME gecijferd met bovenstaande matrix en de optelreeks 12345678. Deze Japanse tekst was in 1941 een zogenaamde open code. Het betekent „Oostenwind regen” en herhaald uitgesproken in het weerbericht waarschuwde het de Japanse missies overzee voor het uitbreken van een conflict met de Verenigde Staten.

H	I	G	AS	H	IN	O	K	A	Z	EA	M	E
40	54	48	18	40	56	74	64	11	00	37	68	35
12	34	56	78	12	34	56	78	12	34	56	78	12 +
52	88	94	86	52	80	20	32	23	34	83	36	47

5.3 Cryptogrammen

MIDWAY-1 3 juni 1942 - 1030 uur

95882 51696 36121 36956 12508 62704 59871 63523 65727 44272 37706
24125 08019 03398 11479 98712 36910

MIDWAY-2 5 juni 1942 - 0400 uur

42023 92773 02297 99276 95325 49562 33133 03729 90760 46371

MIDWAY-3 5 juni 1942 – 0405 uur

08204 50371 90320 52704 26268 76458 53258 76703 36132 10183 35000

MIDWAY-4 5 juni 1942 – 0500 uur46104 08351 28034 78612 68405 46271 04014 19380 08966 25921 53156
27136 88576 94912 52400 03731 90269 04915 72521 76956 21133 05158
65138 62702 93651 74168 22676 41036 85884 33556 36971 64892 35413
06346 68237 44279 08948 59668 90039 93548 61128 05672 41032 35936
21980 51072 70409 64758 47260**MIDWAY-5** 5 juni 1942 – 0530 uur44996 93568 85448 83580 90034 78631 90269 93156 47575 49156 13413
77957 93290 83501 28728 65605 22814 38772 03528 58678 10039 98712
36910

1. Het doel van de opgave is het bepalen van de klaarteksten en van de gebruikte codeertabel. Alle berichten zijn in het Engels.
2. Gegeven is dat de optelreeks uit 10 cijfers bestaat. Bij elk bericht is de optelreeks op hetzelfde punt begonnen. De berichten bevatten alle een geheel aantal groepen van vijf letters. Merk op dat sommige berichten een oneven aantal cijfers bevatten. Dat kan natuurlijk niet in dit systeem. Probeer zelf te bedenken wat er aan de hand is.
3. In de klaartekst zit een tweetal herhalingen. Maar let op! Deze herhalingen zitten verspreid over verschillende cryptogrammen. Spoor die herhalingen op met de in het college gegeven methode en gebruik ze dan om de optelreeks te bepalen en vervolgens te verwijderen. Benut voor deze stap de onderstaande schema's, waarin de codecijfers al op de juiste wijze onder elkaar geplaatst zijn; in bericht 1 is voor de eerste groep van vijf cijfers de bewerking al uitgevoerd.
4. Nadat de optelreeks is verwijderd moeten de berichten ontcijferd worden. Dat gaat gelijk op met het bepalen van de waarden in de codeertabel. Gegeven is dat de lettergroepen in het schema dezelfde zijn als in het voorgaande voorbeeld. Er is echter een complicatie: de rijen en de kolommen zijn *afzonderlijk* verwisseld; d.w.z. zowel horizontaal als verticaal heeft een permutatie van de coördinaten 1..0 plaatsgevonden.
5. Voor het vinden van de juiste oplossing moet worden bedacht wat er bij het afzonderlijk permuteren van rij- en kolomcoördinaten gebeurt met de rij- en kolomcomponenten in relatie tot de getallen die u nu in handen hebt. Neem vervolgens ook de kans mee, dat het waarschijnlijke woord MIDWAY zich in de tekst bevindt. Als u goed geredeneerd hebt, kunt u aan de gestripte cijferreeksen vaststellen op welke positie(s) zich dit woord zou kunnen bevinden.

6. Gebruik die informatie vervolgens om een deel van de coördinaten toe te kennen. Vul de aldus gevonden elementen van de klaartekst in, en probeer via identificatie van woorden en het inpassen van de overblijvende mogelijkheden de gehele codeertabel te reconstrueren.
7. Omdat over het algemeen slechts een equivalente optelreeks gevonden wordt, zal de resulterende permutatie niet identiek zijn aan de oorspronkelijke, maar – in samenhang met de benutte optelreeks – daarmee equivalent. Merk na het ontcijferen op hoe bij overeenkomstige woorden in de klaartekst de keuze bij de verdeling van woorden in letters en lettergrepen is benut voor het bemoeilijken van de analyse.

5.4 Werkschemas

Bekend is dat de optelreeks tien cijfers bevat. *Daarom begint voor elk cryptogram de bovenste regel met het elfde cijfer, terwijl op de tweede regel het cryptogram bij het eerste cijfer begint en de laatste tien cijfers ontbreken.* De cijfers zijn hier per tien gegroepeerd, omdat gebleken is dat daardoor de kans op fouten bij het goed bepalen van de herhalingen geringer is. Op de regel eronder staat hetzelfde cryptogram minus de laatste tien cijfers. Zodoende staan deze regels precies één periode uit elkaar. *Trek de cijfers op de onderste regel volgens het carryloos rekenen van de bovenste af.* Op deze wijze worden de verschilreeksen verkregen, waarin de herhalingen moeten worden opgespoord.

Om het vele werk wat lichter te maken, is een deel van het werk in deze eerste stap reeds gedaan; voor de eerste drie cryptogrammen zijn de verschilreeksen al ingevuld op de derde regel. Alleen voor het vierde en vijfde cryptogram moeten de verschillen nog worden berekend en ingevuld. Dan kan het zoeken naar de herhalingen beginnen, lastiger dan men op het eerste gezicht zou denken. Start daarom de zoektocht maar met het laatste cryptogram ...

bericht 1:

```
3612136956 1250862704 5987163523 6572744272 3770624125 0801903398
9588251696 3612136956 1250862704 5987163523 6572744272 3770624125
4134985360 8648736858 4737301829 1695681759 7208980953 7131389273

1147998712 36910
0801903398 11479
1346095424 25541
```

bericht 2:

```
0229799276 9532549562 3313303729 9076046371
4202392773 0229799276 9532549562 3313303729
6027407503 9313250396 4881864267 6763743652
```

bericht 3:

9032052704 2626876458 5325876703 3613210183 35000
 0820450371 9032052704 2626876458 5325876703 36132
 9212602433 3694824754 3709000355 8398444480 09978

bericht 4:

2803478612 6840546271 0401419380 0896625921 5315627136 8857694912
 4610408351 2803478612 6840546271 0401419380 0896625921 5315627136

.....

5240003731 9026904915 7252176956 2113305158 6513862702 9365174168
 8857694912 5240003731 9026904915 7252176956 2113305158 6513862702

.....

2267641036 8588433556 3697164892 3541306346 6823744279 0894859668
 9365174168 2267641036 8588433556 3697164892 3541306346 6823744279

.....

9003993548 6112805672 4103235936 2198051072 7040964758 47260
 0894859668 9003993548 6112805672 4103235936 2198051072 70409

.....

bericht 5:

8544883580 9003478631 9026993156 4757549156 1341377957 9329083501
 4499693568 8544883580 9003478631 9026993156 4757549156 1341377957

.....

2872865605 2281438772 0352858678 1003998712 36910
 9329083501 2872865605 2281438772 0352858678 10039

.....

Uit de gevonden herhalingen moet een optelreeks worden bepaald. Dat is dan één van de honderd equivalente oplossingen. Omdat meer dan één herhaling kan worden gevonden, is het verstandig om uit beide een oplossing te berekenen. Wanneer het goed gedaan is, wordt tussen alle groepjes van twee cijfers een constant verschil gevonden. Zoals bijvoorbeeld tussen (87 65 99 23 10) en (11 99 23 57 44) het verschil steeds (34 34 34 34 34) is. Dit is van groot belang, omdat bij een verkeerde optelreeks de volgende stap de mist in gaat.

Benut het volgende schema voor het bepalen van het additief uit de encicode van de twee componenten van een herhaling; de ene aan de linkerkant voor de dubbele dikke verticale lijn, de andere aan de rechterkant. Stel het additief voor als ab-cd-ef-gh-ij, waarin elke letter een cijfer van het additief voorstelt. Noteer op de bovenste rij voor elke component van de herhaling deze letters in de juiste vakjes, rekening houdend met de positie van de herhalingen in het cryptogram. De dubbele verticale lijnen herinneren er aan dat het additief een periode van vijf dinomes (is tien cijfers) heeft. Het additief begint in het algemeen voor elke component van de herhalingen op een andere positie, denk daaraan. Vul op de derde rij de cijfers van de encicode in. *Let op, gebruik de cryptogramcijfers van de tweede regel ter plaatse van de herhalingen voor deze bepaling.* Begin nu met de eerste dinome van het additief in de linkertabel op nul te stellen (is al reeds ingevuld in de tabel). Vul de bijbehorende dinome van de klaartekstgroep in op de vierde rij en vul die ook in op de juiste plaats in de rechtertabel. Bereken daaruit de dinome van het additief ter plaatse en zet die weer in de tabel aan de linkerkant waardoor weer een dinome van de klaartekst wordt gevonden, enz.

	component-1					component-2				
additief a-j										
additief 0-9	00									
dinome										
encicode										

Als het additief is gevonden, kan het strippen van de encicode beginnen. Daarvoor dient het onderstaande schema. Op de bovenste regel staan de cijfergroepen van het cryptogram (de encicode), ditmaal opgesplitst in de dinomes van de onderliggende vercijfering. *Schrijf de tien gevonden optelgetallen van het additief herhaald op de tweede regel en zet daaronder op de derde regel hun verschil, d.w.z. **trek de onderste van de bovenste af.*** In elk cryptogram is de eerste dinome vercijferd met de eerste dinome van het additief, enz. Uit de vorige stap is natuurlijk bekend geworden wat de eerste cijfers van het additief zijn.

Let op. Het is werkelijk belangrijk om het verschil te nemen en niet de som. Alleen zo (encicode-additief=dinome) vindt men de oorspronkelijke vercijferde klaartekstgroep terug. De reden hiervoor is gelegen in de vier combinaties die mogelijk zijn door de keuze van additief/subtractor en optellen/afrekken. Van die vier combinaties zijn er twee goed en twee fout. (Hier moet men of aftrekken of het complement van de gevonden oververcijfering optellen.)

De laatste stap is het ontcijferen en de daaruit volgende reconstructie van de codeertabel. De onderste regel in het werkschema is bestemd voor het noteren van de klaartekst. Gebruik de blanco codeertabel voor de oplossing. Zet in elke cel de bij die coördinaten behorende klaartekstgroep.

bericht 1:

95 88 25 16 96 36 12 13 69 56 12 50 86 27 04 59 87 16 35 23 65 72 74

.....
.....
.....

42 72 37 70 62 41 25 08 01 90 33 98 11 47 99 87 12 36 91

.....
.....
.....

bericht 2:

42 02 39 27 73 02 29 79 92 76 95 32 54 95 62 33 13 30 37 29 90 76 04

.....
.....
.....

63 71

.....
.....
.....

bericht 3:

08 20 45 03 71 90 32 05 27 04 26 26 87 64 58 53 25 87 67 03 36 13 21

.....
.....
.....

01 83 35

.....
.....
.....

bericht 4:

46 10 40 83 51 28 03 47 86 12 68 40 54 62 71 04 01 41 93 80 08 96 62

.....
.....
.....

59 21 53 15 62 71 36 88 57 69 49 12 52 40 00 37 31 90 26 90 49 15 72

.....
.....
.....

52 17 69 56 21 13 30 51 58 65 13 86 27 02 93 65 17 41 68 22 67 64 10

.....
.....
.....

36 85 88 43 35 56 36 97 16 48 92 35 41 30 63 46 68 23 74 42 79 08 94

.....
.....
.....

85 96 68 90 03 99 35 48 61 12 80 56 72 41 03 23 59 36 21 98 05 10 72

.....
.....
.....

70 40 96 47 58 47 26

.....
.....
.....

bericht 5:

44 99 69 35 68 85 44 88 35 80 90 03 47 86 31 90 26 99 31 56 47 57 54

.....
.....
.....

91 56 13 41 37 79 57 93 29 08 35 01 28 72 86 56 05 22 81 43 87 72 03

.....

52 85 86 78 10 03 99 87 12 36 91

.....

Codeertabel voor oplossing										
	1	2	3	4	5	6	7	8	9	0
1										
2										
3										
4										
5										
6										
7										
8										
9										
0										

Hoofdstuk 6

PRACTICUM – Alfabet reconstructie

In deze oefening wordt een alfabet gereconstrueerd uit isomorfen. De methodiek voor deze reconstructie is te vinden in de syllabus, in het hoofdstuk Cryptoanalyse.

Opgave 1

In het cryptogram van een tekst die is vercijferd met een progressieve Vigenère met gemengd cijferalfabet zijn enkele isomorfen gevonden. Hiermee kan dit cijferalfabet worden gereconstrueerd.

isomorf-1	isomorf-2	isomorf-3
JPPXLPWAHYEH	ZLVXLHEAHIOFUMASX	ZMNOHSMGLQ
WEECUEIQPJLP	YKNVKJIGJCTQZAGUV	GJBZRMJQSX

1. Leg de kettingen verkregen uit isomorf-1 horizontaal (van links naar rechts) en combineer deze verticaal (van boven naar beneden) met de kettingen uit isomorf-2.
2. Bouw zoveel als mogelijk van de beide isomorfkettingen aan elkaar en breng daarmee een zo groot mogelijk aantal letters op één rij. Met deze twee isomorfen kunnen 16 van de 26 letters worden geplaatst.
3. Gebruik vervolgens isomorf-3 om het alfabet compleet te maken. De letter D komt niet in de isomorfen voor, maar kan op de overgebleven plaats worden ingevuld.
4. Onderwerp het gevonden alfabet dan aan decimatie 11: dat wil zeggen, steeds elf letters verder tellen in het gevonden alfabet en die letter achter de vorige schrijven. Als het resultaat achterstevoren lijkt te staan, is dat het gevolg van de andere manier van decimeren, namelijk steeds de volgende letter uit het gevonden alfabet elf plaatsen verder noteren. Die manier van doen is equivalent met decimatie 15 in de eerst aanbevolen werkwijze. Met welke letter wordt begonnen is niet van belang.
5. Na decimatie resteert een alfabetpermutatie waarin gemakkelijk een kolomtranspositie kan worden herkend. Los deze op en bepaal zo het gebruikte sleutelwoord.

Opgave 2

De volgende opgave komt uit een Engelse cursus cryptoanalyse van 1942. De isomorfen zijn het resultaat van een vercijfering met de Wheatstone cryptograaf. De gehele tekst van deze cursus is te vinden in *A Course in Cryptanalysis*, een reprint door Aegean Park Press van *S.I.Course, Revised and Enlarged, June, 1942*.

Hieronder staan vijf isomorfe vercijferingen van de erboven staande klaartekst (niet van belang voor de reconstructie). Bepaal voor zover mogelijk uit deze isomorfen het cijferalfabet. Omdat niet genoeg materiaal voorhanden is voor het gehele alfabet, blijft de positie van 3 letters onbekend.

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

Opgave 3

Tot slot uit dezelfde bron als de vorige opgave nog twee oefeningen in decimatie. Beide zijn gebaseerd op een sleutel.

YRALHCGMQZINEWDJOXBTUSVFKP
PIGTNSJWEBLYDFQAVHUZOKXRCM

Hoofdstuk 7

PRACTICUM – Kerckhoffs superpositie oplossen

Deze oefening is een vooroefening voor de analyse van de Hagelin cryptograaf. In het werkschema is het begin van twintig in Beaufort gecijferde Engelse berichten gegeven. Deze moeten worden opgelost en de sleutel bepaald.

- De berichten zijn gecijferd met de U.S.ARMY-disk. Dat levert een Beaufort substitutie op. Gebruik de (gewone) Beaufort tabel achterin of die in de syllabus. De gecijfersleutel is een doorlopende sleutel (running key). Het is dus geen periodieke maar een aperiodieke sleutel. Alle berichten hebben hetzelfde startpunt in de sleutel.
- Als eenmaal een begin van de ontcijfering gevonden is, kan aan de woorden van de berichten worden doorgebouwd. Omdat de woorden van verschillende lengte zullen zijn, is er altijd wel een volgende letter die goed geraden kan worden. Uit een goed geraden letter volgt de bijbehorende letter van de sleutel, enzovoorts. Ook kan het vervolg van de sleutel soms worden afgeleid uit het reeds gereconstrueerde deel.
- *Voor het maken van een entree in de cryptogrammen kan het best worden begonnen met de eerste twee letters van de cryptogrammen.* De volgende tabel maakt dit gemakkelijk doordat voor de eerste twee letters van de cryptogrammen alle mogelijke ontcijferingen zijn gegeven. Op elke regel staat vooraan een sleutelletter gevolgd door de ontcijfering van alle letters die als eerste en tweede letter voorkomen. In de kolom onder de # staat het aantal ontcijferde letters uit de groep ETAONIRSH, d.w.z. het aantal ontcijferingen in de groep van meest voorkomende letters.
- Het aantal verschillende letters op de eerste twee posities is gering. In de eerste letters van de twintig cryptogrammen komen zeven verschillende letters voor en als tweede letter zelfs maar vijf. Het ligt in de verwachting, dat dit hoofdzakelijk veelvoorkomende letters zullen zijn. Zoek dus naar die sleutelletters, die veel van deze letters en ook nog goed ogende combinaties produceren. Bovendien zullen de beide sleutelletters dan waarschijnlijk ook een goed digram vormen.
- Kijk naar de kolommen met de tweede letter: sleutelletter O oogt goed omdat alle vijf klare letters dan tot de groep ETAONIRSH behoren, evenals de sleutelletter zelf. Gebruik de frequentietabel Engels om veelvoorkomende digrammen te vormen met de letters uit de eerste kolom. Kijk of in alle berichten met de gekozen eerste sleutelletter de twee beginletters een passende ontcijfering krijgen.
- Als eenmaal een goed begin is verkregen, gaat het ontcijferen bijna vanzelf. Deze opgave illustreert duidelijk hoe belangrijk het is om zulke superposities te vermijden.

1e letter	2e letter						
	A	B	D	N	O	W	Z
A	A	Z	X	N	M	E	B
B	B	A	Y	O	N	F	C
C	C	B	Z	P	O	G	D
D	D	C	A	Q	P	H	E
E	E	D	B	R	Q	I	F
F	F	E	C	S	R	J	G
G	G	F	D	T	S	K	H
H	H	G	E	U	T	L	I
I	I	H	F	V	U	M	J
J	J	I	G	W	V	N	K
K	K	J	H	X	W	O	L
L	L	K	I	Y	X	P	M
M	M	L	J	Z	Y	Q	N
N	N	M	K	A	Z	R	O
O	O	N	L	B	A	S	P
P	P	O	M	C	B	T	Q
Q	Q	P	N	D	C	U	R
R	R	Q	O	E	D	V	S
S	S	R	P	F	E	W	T
T	T	S	Q	G	F	X	U
U	U	T	R	H	G	Y	V
V	V	U	S	I	H	Z	W
W	W	V	T	J	I	A	X
X	X	W	U	K	J	B	Y
Y	Y	X	V	L	K	C	Z
Z	Z	Y	W	M	L	D	A

Ontcijfering van de eerste twee letters.

WERKSCHEMA

- | | | | | |
|--------------------------------|-------|-------|-------|-------|
| 1. BKGWH EZLSI FQPSS GYKXS | | | | |
| 2. ZOCAG EKAAB HNDMZ PMWVW | | | | |
| 3. DXYCP EJLER HNKGE ZIZDK | | | | |
| 4. OBISV GMJSI QGMEZ CNDWG | | | | |
| 5. BKXQC PMTHR HMHEH ATKWR | | | | |
| 6. ZHVAP HMLZT WWNRA FWGBF | | | | |
| 7. OOKXB EKLEC FQPSS GYKXO | | | | |
| 8. BKWKP QTTER HLTQF FWKDG | | | | |
| 9. NXIMM PVQEE PITTH CXZDK | | | | |
| 10. WHIRX ABTWP GAKAH LXTKH | | | | |
| 11. AKZBC EIRNF QCXSO GIWOR | | | | |
| 12. AKRAG PFZKP WBBNZ LQDKT | | | | |
| 13. BKGKI IVQRB DNGEZ LNBSC | | | | |
| 14. ZHVQZ CFQYA OXXRK NUVOZ | | | | |
| 15. BKHAC EZCOV TTKNS QTABW | | | | |
| 16. BKUAC NIEGH NRTLK FOSGZ | | | | |
| 17. DXIPT RILET OLBCI TIABG | | | | |
| 18. OBTWC ELNKN HBXMZ TWJHK | | | | |
| 19. BKXQC POQYC SQJWZ LNBWK | | | | |
| 20. AKRAC IBPSA QQQMB PMAXR | | | | |
| s: ?????? ?????? ?????? ?????? | | | | |

Hoofdstuk 8

PRACTICUM – Hagelin oplossen

Deze opgave bouwt voort op de voorgaande Kerckhoffs-opgave. Acht berichten in het Nederlands zijn gecijferd met een Hagelin cryptograaf van het type M209. Het systeem is dus Beaufort, maar wel met de aangepaste tabel (zie achterin het werkboek en in de syllabus).

- Het oploswerk bestaat uit verschillende stappen. De eerste stap is het *in diepte* leggen van de berichten. Zodra dat is gebeurd, hebben we dezelfde situatie als in de vorige oefening: een Kerckhoffs superpositie. Oplossen daarvan levert een sleutelstroom in de vorm van een rij getallen, overeenkomend met het aantal stappen bewerkstelligd door de draaiende kooi met linealen en ruiters.
- Constateren of twee berichten in diepte kunnen liggen kan als volgt:

```
TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN QMDPO PBQGL GVMKH
TYDYJ JMYNY HUZVW CNVQJ UGMXW LWKVT ZEXVV XSXRC DWIRS UZLTX MERTK PKVDT PBQJ ZHCKH
xxxxx xxxxx xxxxx .x... .. .x... xx... .. xxxx. ...xx

TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN QMDPO PBQGL GVMKH
>TYDY JJMYN YHUZV WCNVQ JUGMX WLWKV TZEXV VXSXR CDWIR SUZLT XMERT KPKVD TPBQG JZHCK
>.... x.... ..x. ....x. .... ..x.. .... ..

TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN QMDPO PBQGL GVMKH
>>TYD YJJMY NYHUZ WCNVQ QJUGM XWLWK VTZEX VVXSX RCDWI RSUZL TXMER TKPKV DTPBQ GJZHC
>>... ..x. .... ..x. .... ..x. .... ..x....

TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN QMDPO PBQGL GVMKH
>>>TY DYJMM YNYHU ZVCN VQJUG MXWLW KVTZE XVVXS XRCDW IRSUZ LTXME RTKPK VDTPB QGJZH
>>>.. .... ..x. .... ..x. .... ..x
```

Hierboven zijn het begin van het eerste en tweede bericht onder elkaar gelegd. Vervolgens zijn ze onderling steeds een plaats verder uit elkaar geschoven. De kruisjes geven de coïncidenties aan. Het grote aantal coïncidenties op de bovenste superpositie maakt het meer dan waarschijnlijk dat deze berichten al in diepte liggen en de sleutelstroom dus voor beide berichten op hetzelfde punt gestart is.

- Als de diepte voor dit tweetal berichten gevonden is, hoe staat het dan met de andere berichten? Om dat te bekijken is het begin van alle acht berichten onder elkaar geplaatst. *Markeer de posities met drie of meer coïncidenties en trek zelf je conclusie.* Kun je uitrekenen wat de kans is dat drie of meer coïncidenties voorkomen wanneer de acht berichten in diepte liggen? En hoe groot die kans is als dit niet het geval is?

TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN QMDPO PBQGL GVMKH
 TYDYJ JMYNY HUZVW CNVQJ UGMXW LWKVT ZEXVV XSXRC DWIRS UZLTJ MERTK PKVDT PBQJ ZHCKH
 HVUXP HCMCF YTVLG VOFUD ZJWSG MTBQF FYTFV STWRM PRUAD CIGMB PXEPA UYQFI RTZGZ GRQWG
 UIBIY PQHSQ QPWOV BHUZS USBKZ CUJYY WPSPE SHIVV MTQYT QCXXC EOEOY GRTXO WYZMU AWAKV
 QYRON MMFYK HUWAZ GENLO UMBKU INWZT YPNZB BGBAF MATAD YHBOJ XIZFP PLKKJ NBEGP NBQLM
 TYDJX WHTTK DJWRC GJHYV HXQKM WOFPG VLSQA WVPSM MQESQ XZOCE TVNAO GRTPS QGHBC JHLCQ
 OPDQX KQYBF YTBMP PBIFX WFLLT LBBWP KIWWX WNOAI YWUNM BZSTV NXEVI PRCXK NSZGR LDNOV
 TYDHT XADKB JWVTD ZCMLJ USBPZ COXKB BFDFJ XNKIR PRTHM ENFRZ TJJAN PDWPX WYDFJ KQQPM

- o Met alle berichten in diepte geplaatst moet nu de klaartekst worden bepaald d.m.v. de *Kerckhoffs superpositie*. Alle berichten zijn in het Nederlands. Er zijn meerdere tactieken voor het vinden van de oplossing mogelijk. Bijvoorbeeld beginnen met de eerste letters van alle berichten, op dezelfde manier als in de vorige opgave. Een andere tactiek: op posities met drie of vier dezelfde letters is die letter een goede kandidaat voor de Z die hier als spatie is gebruikt of voor de E. Kijk wat de andere letters opleveren en als dat er goed uitziet, probeer dan of de E's misschien deel uitmaken van veel voorkomende combinaties als EN, DE, HET, EEN. De andere berichten leveren de feedback voor de geloofwaardigheid van die aanname. Zijn eenmaal een paar herkenbare woordfragmenten gevonden, dan is het afmaken van de oplossing een fluitje van een cent. Extra informatie is beschikbaar in de vorm van bijgaande, halfverkoelde papier-snipper die werd gevonden in een asbak naast het blad met de gecijferde berichten. Deze aanwijzing kan helpen om de klaartekst van de berichten te vinden.



- o Als het gelukt is om de berichten te ontcijferen, dan is ook de reeks sleutelgetallen (het aantal kicks) ter beschikking gekomen. Merk wel op dat er een onduidelijkheid overblijft, want tussen 0/26 en 1/27 is nog geen onderscheid gemaakt. Deze opgave is echter zo geconstrueerd dat kicks van 26 en 27 niet voorkomen. Ware dit wel het geval geweest, dan was dit bij het invullen van het eerste werkschema snel duidelijk geworden: in een kolom met hoge waarden voor de kicks vallen een 0 en een 1 zodanig uit de toon dat correctie naar 26 en 27 min of meer vanzelf spreekt. Met de gevonden

sleutelreeks gaan we verder naar fase twee. Het reconstrueren van de instellingsparameters: te weten het aantal ruiters op de 27 linealen en de stand van de 131 pinnen op de wielen. Een aantal werkschemas vergemakkelijkt de tamelijk omvangrijke uitwerking van deze opgave.

- Om het werk wat te beperken is het 26-wiel niet meegenomen, d.w.z. voor dat wiel zijn geen actieve ruiters aanwezig. Begin nu met het 25-wiel te analyseren. De diehards proberen ook minstens één andere wiellengte om het verschil te zien. *Schrijf de sleutelreeks per 25 op een regel en bereken voor elke pinpositie van het 25-wiel het gemiddelde van de lineaalverschuiving.* Met de opeenvolgende sleutelgetallen horizontaal uitgeschreven is dat dus het gemiddelde over de kolommen.
- Maak een histogram van deze gemiddelden (afgerond op gehele getallen) en stel vast of de verwachte tweetoppige verdeling aanwezig is. *Leidt uit het verschil tussen het maximum van de twee toppen af wat het meest waarschijnlijke aantal ruiters op dit 25-wiel zal zijn en bepaal welke pinnen aan en welke uit staan.*
- *Trek vervolgens voor de posities met een pin die aanstaat het aantal veronderstelde ruiters af van de betreffende sleutelgetallen.* Dit levert effectief een reductie van de machine tot een waaruit het zojuist geanalyseerde wiel is verdwenen. Herhaal dit proces voor het 23-wiel.
- Voor de resterende 21, 19 en 17-wielen blijven dan zo weinig ruiters over, dat ze gezamenlijk kunnen worden geanalyseerd. Gebruik hiervoor het laatste werkschema. *Vul op elke positie met een overgebleven kick van 0 de nullen in en herhaal voor elk wiel deze nullen verschoven over de respectievelijke wielperiode.* Op de posities met nulpinnen voor twee wielen wordt de kick van het derde wiel zichtbaar.

Cryptogrammen

HAGELIN-1

TYDYJ JMYNY HUZVW DNZVK YDTRA TFYKU FYKJH SPGVM FWWNW UZBGA KCUEN
 QMDPO PBQGL GVMKH DEHGP JLBBN MWPYS JCWPR XLORR UFSFB JKOGM MERWZ
 PDWGU DCRUT UPYOX KRQTR AHTRV LAHJY VZRPC QQHIO LCTDR OHWZY QJSKL
 PWVXS QSDWK JEBMF PGOOH RZCKL OYVHV WQGGX WACTX ICGWA HFUKM TJHCR
 OIWOE VERA DASSI PFCHS NPVFP LUVWH RSEOH VOUFK XETOH RUPLO MAGFS
 NCQTO NEOWF NOHBC GEQQD MYWKD DAOFJ YTSWX WCAOD JYZNI ONPRJ ZJFJZ
 TJUJL CDHAQ QUTNB YHVWK TJSIK KHSXL ZZAGE YOHOG MBYJP KZNGE JYYSN
 YUVZI ITBUJ YNCRZ POGJJ INQOB XXRAD OLMKT YUPVD XCYWK VKAWR ECIQV
 JETRI ZBCAU SHXVA TIZEA XDCWV RXNCO ZLUGP VSPNI VTILB LWOQN FFAII
 VQHTM HAOHL OFYIH FLZGK FLIRC QBFZM OTOOW RHOLK QBGSV PGEWM KRJUG
 KZWCA PPTGD KUTDE UIZ

HAGELIN-2

TYDYJ JMYNY HUZVW CNVQJ UGMXW LWKVT ZEXVV XSXRC DWIRS UZLTX MERTK
 PKVDT PBQJG ZHCKH LITVL PMOFA FRQUM NHUAE LCITA RHQDB BYMER XNZLC
 HMFESK JBSAS EXOYO PBUAO JQTDI KANQZ HUZEB CSMLK UDDJN CGJUP SOJPC
 SRIPY GMPNV DATCP GNJCM EZTXK NGQJQ VXGGB QMKQI PJKCB SFUVU TGMNG
 BCABW IPDZW YMNSV KLXTX JKWPO YBQBH SBESS MFUFK MUZRL UZCLS REKVD
 ZFBCA GVEMV NCLXC BDMDU HIIZM HLARC MTOHA CLRTC UMADC UYSBC MNGRI
 TYZPL YSAWF LZFIJ OTEWF RJSIK UCXSR YO

HAGELIN-3

HVUXP HCMCF YTVLG VOFUD ZJWSG MTBQF FYTFV STWRM PRUAD CIGMB PXEPA
 UYQFI RTZGZ GRQWG XBDVV PXGAF BWPYS NJMKR LPHXY JJYDZ SKRZQ FJXSE
 SZSBH ELQCS LPNTB VGEVS UTHNP FRDEV CUMPE XMBIR KAHPN GQSUL MJBQU
 URKOG OBLQM VJTWL ALHQW TPKKL ZMMJQ GFGWX LFOHX AXVLN LFBVA RUILA
 UWYTA WWMLW TBMVF VHOCM NHVKI GBEVY RSEHT TZRSJ EZHET ITPWF DMLGY
 NRPCP JVREO WNSUR PMRBD QQOZZ BMHKO FNEJY LTYLI UMCXI UDCQY DIFXR
 RTAMM DHGBG UZXIY ISPUK PVGBT CZSCH NWCJQ TWQUH MMIFF KNXVY ZDOJO
 KABJX MRMES EJIBZ TBPUD BTBXP SCMBP ZQTIY EDFEG EKCXQ RKNEM CBBBC
 XKOOI LOPGC KTKLW

HAGELIN-4

UIBIY PQHSQ QPWOV BHUZZ USBKZ CUJYY WPSPE SHIVV MTQYT QCXXC EOEYO
 GRTXO WYZMU AWAKV YWBNB PTJAJ YCTQS TUCPB CRWIL WRVQW SQMTQ MSYXK
 AHWZF KQVZJ FPZVY PYDVM UQENV UEUEV HOYTI XHMNR GYTJI XMRZH LAGCZ
 NCRBI UNDWV VFBVT GUHHT RZVKL TFQKL YGGZR DNKMT ORZLN ZJHWO EFHUG
 JIXWF SOREM TOQNS TBTET IPDRS WBQKO BUTGM YLFWB EYHSD GHTCK QLBHC
 BBRAZ YRHLA SNRHD TMMCD GNYVF NVHKJ PIZZU VXTJC OSDGR WYSAP ZMJVJ
 XMDCF XSVQF LZABV KNZWK ITSQY BFSRL LZWGE UKHFM XBNGU KRIBB TYPJH
 NJKUC HAXKL GIBGE PIAHN TTQXU JRAIW VEPIR ELWJB MXYBQ UGEYD JGCBO
 FDSDE ZJYNO WHXVY YIUFA LFTPJ VFUFC

HAGELIN-5

QYRON MMFYK HUWAZ GENLO UMBKU INWZT YPNZB BGBAF MATAD YHBOJ XIZFP
 PLKKJ NBEGP NBQLM TAFTK ZIOYO BVYGM IPJTV XLLLY DQFYG DFTNU DMMJM
 NDZGB KQLXW YIDYU BMIWN OELEL HEEBT QRUPQ WMYFA QPDYN FUVHD WWRZO
 PRSXT USDPN QLCBT GUVAH IVMON TTGIY QKMFS WVXMB OXZMA ZEZSB XUWVH
 UPXAE EPCLQ TJYSY TURGX YXSGB QKDWO TXMIL NFCOF PPXQM ZFEQO CXXVW
 IZQUN EWCVA YCFUC FRNVX TDQZM UFAQX WSAQR LSODD NFRSN AYKJC LNEEP
 GDLYD QHVNK LUMIC TTZDF KOSNM PVDWV

HAGELIN-6

TYDJX WHTTK DJWRC GJHYV HXQKM WOFPG VLSQA WVPSM MQESQ XZOCE TVNAO
 GRTPS QGHBC JHLCQ TMIKA IOJLU DRKZR ZJQDV ELVLC PFOUF WDDHU DSNKS
 WMVRS YLGGX VKLKK PXUAS RSHZK CMCJF PLVPI QBXNV GHWIZ VVSUD IFOZR
 CNRPH UAWVV VYTNE PCJCM JZCKL PMRWW KGBKX CPTDK ZCLJF RFOKH TYXEO
 OGIBJ VBLAL YHUDQ TPNXX IERTL LXAKZ GGAGM JUTOW WAHEZ TWNWK NDKPH
 YVNNW GHNHU SHYSR PMRBL BPMDY WRADX PZTKQ XRHJC OPNZC OKQON ZVVPX
 TGIPZ QIISF ULZQH FNVDK ONSNX XFXGG ZETGL TWQKH FJZOV UB

HAGELIN-7

OPDQX KQYBF YTBMP PBIFX WFLLT LBBWP KIWWX WNOAI YWUNM BZSTV NXEVI
 PRCXK NSZGR LDNOV KCATP KZNWO KRQZ NWESR GSCMD RQKIB XVTNC IHCGS
 NUDGO XCLMS FPHZA XOHZO OPIFG GMPV PFQPW XNTGV PUMHM WVRLD IJGAT
 CVUOG KBVAT MMIXT JPOMX IJAKL ZLBOL KYRDC BXLWC BRZIA FKAFC TUTRC
 UKWOF OKGYW YZYL F CKXTX RGMGF WJWU NZEYD BPKOW PCRSI PAYJF GXWVD
 XPRNS QEDCO OHFKM HMRAE HOCDR QLBJD PUOHV CE00J FIZSA FYSAP FQBVX
 PRMGL CRZJB ZUOZQ FCXFW YABBT BOJQZ NOMXY

HAGELIN-8

TYDHT XADKB JVWTD ZCMLJ USBPZ COXBK BFDFJ XNKIR PRTHM ENFRZ TJJAN
 PDWPX WYDFJ KQQPM BRIFO CWONN YPLOR AYVPU CBWIL WIVYC SWHLK CANYV
 KZQFB GLXUH EBJON GWIWN OOXEL PRHBI LHGAW BYKVT CYWDY TQEZV HUGYP
 NCWLT BBDKA IWOXF APWQP GSNLU TWQFX VWBFU XHRHF ERUQI QYIQJ GZFOD
 JBUWR WKXET PCMQF YUTXO GKILE AGRJU ROVGH BZOEX CIMRL TWYCB MSWPV
 IFZNS GHZJJ GBNHD TCVLH VDXQM FEJWD DIHUF UGPBH AINAN AWKJC LNQIG
 TKMUL CMWWK OHKDJ AUDHC EOQNK VOTGX FDGES YFXTY SREAP GGNWM FRXWT
 KJFAR YOKKJ SZKZH GCMT C UXVZV

WERKSCHEMA WIEL 25																									
positie	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
kicks																									
kicks																									
kicks																									
kicks																									
kicks																									
kicks																									
kicks																									
kicks																									
gemiddeld																									
kicks 25																									

HISTOGRAM WIEL 25																												
8:																												
7:																												
6:																												
5:																												
4:																												
3:																												
2:																												
1:																												
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

WERKSCHEMA WIEL 23																							
positie	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
kicks																							
kicks																							
kicks																							
kicks																							
kicks																							
kicks																							
kicks																							
kicks																							
gemiddeld																							
kicks 23																							

HISTOGRAM WIEL 23																											
8:																											
7:																											
6:																											
5:																											
4:																											
3:																											
2:																											
1:																											
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

WERKSCHEMA WIEL 21, 19 en 17																			
positie	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
kicks																			
21																			
19																			
17																			
positie	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
kicks																			
21																			
19																			
17																			
positie	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
kicks																			
21																			
19																			
17																			
positie	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
kicks																			
21																			
19																			
17																			
positie	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
kicks																			
21																			
19																			
17																			

Hoofdstuk 9

WEDSTRIJD – Uitdagende opgaven

9.1 Kies een opdracht

Voor de eindopdracht wordt gekozen uit de volgende mogelijkheden.

In de *Drugs-oefening* moeten cryptogrammen in verschillende systemen worden opgelost. Als complicatie is niet gegeven in welk systeem een bepaald cryptogram is vercijferd. Deze opgave is over het geheel genomen niet zo moeilijk.

In de *Normandië-oefening* is sprake van meer dan een systeem, zowel substitutie als transpositie komen aan bod.

In de *PearlHarbour-oefening* is sprake van één enkel systeem, maar de cryptogrammen zijn verdeeld over verscheidene cryptoperioden waarin de sleutel wordt gewisseld. Deze opgave is beduidend lastiger, omdat er in een combinatie van twee systemen is vercijferd.

In de *NoordAfrika-oefening* zit een oververcijferde code. Het voornaamste doel is om de oververcijfering grotendeels te ontraadselen. De reconstructie van het codeboek is met de geringe hoeveelheid materiaal maar voor een uiterst klein deel mogelijk.

9.2 Drugs oefening *

Inleiding

Deze oefening is gesitueerd in de drugshandel. Vanzelfsprekend bestaat er geen enkele gelijkenis met bestaande personen en situaties.

De moeilijkheidsgraad van de systemen waarin de berichten zijn gecijferd is wisselend, de meeste zijn tamelijk makkelijk, maar eentje is vrij lastig. Ook wordt niet precies verteld welk cryptogram in welk systeem is gecijferd. Eigenlijk zou het nog realistischer zijn om helemaal niets te vertellen over de systemen die kunnen worden verwacht, maar dat maakt het misschien te moeilijk; het is nu al niet zo eenvoudig voor beginners. Gedacht mag worden aan eenvoudige substitutie, transpositie, polyalfabetische substitutie met normaal en met gemengd alfabet en een voortschrijdend gemengd alfabet met stappenpatroon.

Voor het laatstgenoemde en moeilijkste systeem zijn een paar hints wel op z'n plaats. De start van de oplossing kan worden gevonden door de twee bruikbare isomorfen op te sporen; deze kunnen, zoals bekend mag worden verondersteld, het cijferalfabet opleveren. De volgende fase is misschien nog lastiger: het bepalen van het stappenpatroon en in relatie daarmee de periode van het cryptogram.

Vanuit Amsterdam opereert een internationaal werkend drugssyndicaat met vertakkingen naar Azië en Spanje. De politie heeft op verschillende manieren (afluisteren van radioverkeer, medewerking van KPN) een aantal gecodeerde berichten in handen gekregen. Het onderzoek staat onder leiding van hoofdinspecteur Henk Heroinejager. Henk heeft uw hulp ingeroepen om deze berichten op te lossen en te vertalen in klaartekst. Hieronder volgt alles wat Henk tot nu toe te weten is gekomen over de bende.

Uit een oriënterend onderzoek concludeert u al snel dat voor de verschillende links in het netwerk steeds een ander geheimschrift is gebruikt. Henk zal in het bijzonder geïnteresseerd zijn in het bericht aan de Grote Baas, omdat hij hoopt daardoor diens identiteit te vinden; dit cryptogram zal wel in het moeilijkste systeem zijn gecijferd.

De dramatis personae zijn:

- Karel Doorzijker. Bijgenaamd de braller. Rondreizend inkoper met Zuidoost Azië als werkterrein, voornamelijk opererend in de zogenaamde Gouden Driekhoek.
- Mina Janine van Drotten (Mientje). Secretaresse op het Amsterdams hoofdkwartier van de bende.
- Gijsbert Schrevelaer, bijgenaamd de rokkenjager. Zaakwaarnemer van de Grote Baas. Leidt vanuit het hoofdkwartier in Amsterdam alle operaties.
- De Grote Baas. Echte naam onbekend. Woont aan de Spaanse zuidkust. Onderhoudt contact via poste restante adressen in Tarragona en Fuengirola.
- Jan Karel Gompers. Beheerder van het filiaal van de bende in Bangkok. Weinig over bekend.
- Achmed al Moussaki. Bijgenaamd de Mahdi. Leider van een in Libanon zetelend syndicaat waarmee min of meer vriendschappelijke relaties worden onderhouden.

- Greet Zeelander. Koerierster.
- Monique Bronovo. Koerierster. Undercover agente van Henk Heroinejager. Nog maar kort in de bende. Aantrekkelijk type.
- NN. Naam onbekend. Kontakt van de bende bij de luchtbevrachting op Schiphol.
- Guus Hannekemaier. Radiotelegrafist op het smokkelschip de POPPYCOCK, varende onder Panamese vlag. Staat merkwaardigerwijs in de bende in rang hoger dan de kapitein van het schip.
- Jan Geluk. Freelance drugsdealertje in de Amsterdamse binnenstad.

De cryptogrammen staan in willekeurige volgorde van moeilijkheid. Alle teksten zijn in het Nederlands.

Berichten

DRUGS-1 van: Gijs Schrevelaer aan: Jan Geluk

CNQ XAQTXM JSSG SSQ OSQXAM DSISGSQ TUPE XSOSDYXS WPQXAUAST NDT
IPGAMS CSSG TUPE VSISTUAM PE MSVGHACSDABCS RNQASG TUPE NYDSISGAQM
ONUSGXNM AQ XS GPXS ZNNQ UHTTSQ UJSS SQ XGAS XPPG RPQAFHS TUPE
VDABY RSU BS EPUSQ INQ ZNNG NY TUPE MABT TUPE

DRUGS-2 van: Poppycock aan: hoofdkwartier Amsterdam

XKEKQ VUTXO XNMPE QBDCU IKNEQ TDZET BSRMJ JOQHQ SFFLY JTCLF INYXV
NKWHH SSCHD SXKEK QGKHX KGYKS UGVMQ YDSEK WERMW FIIZB CROTN WEIEP
WOMXW PNAQA DTAKS MENSE

DRUGS-3 van: Poppycock aan: hoofdkwartier Amsterdam

QKHCS MYPJC AVPHU PNFEV VLNDX CDTAA JWDLU RXRAF ODARX KHLRM DFIIZ
BCROL NCVIC PMCPD AMCYX XPMEE UGVMY ULMEC IBXXX

DRUGS-4 van: Poppycock aan: hoofdkwartier Amsterdam

IDUEV NCVZD SXOTJ AYPCK DQIUR PUQTW DKLZX TJZBN NISLY LTOPW ADOLG
POIYL NCNSD LFSME WAPIH KJNSK DINWN BERHR EPDYZ SXWRZ CUKAV OAJDM
PPNAS VNTEE QRKSU GVMZA ALYUI YMNTC VDEGI CSPAP TQADT TIKSE TCJER
YRCFK VTNAS LYLTO PIBPN HLPFX CDTYO UZMPP NXXXX

DRUGS-5 van: Poppycock aan: hoofdkwartier Amsterdam

SKPDA YPCKD QILPD TMADH KJFAP EAENS EXRFF PTRAI YXFDA AVPLZ AQDML
 IPKOQ NUTDN DNFRK VNIOQ AMPPN TRTMP XSLNZ RKOPW ABMMR XIBSN UPXND
 NCPEK NDSCD QECIB GDTTK KDNEP RLLAC QADTJ TOGMF FYHSI LOGLP TCCMR
 WPEKD TWSXX RFGJO PMWUO DQPDT JLENS EBDIK ESKGT DELQP AHPLF TSEDP
 QOWZR LPDAD TVBXC RZTCC HDYPS LIYEA IIVYP PELVM TVSDT UROEN CHYHS
 VTYPB LAHYH SFFPC DZWSH DRBRU LLYEA IIQRK RPEYS VXEWI FXCDT YOUZM
 PPNXX

DRUGS-6 van: Poppycock aan: hoofdkwartier Amsterdam

FFPCR WFSYK ANWRD RYPIA BDTDP YJNID XBTPA PMRAD TJPHI KCPQH TCQZG
 VBEDL RYTJA LIKXX SPTWX OMPPN GJADT JHIND XCRTM TJORM DEKBM EVASL
 YLTOP ITUIS ARURP URQCX DBWPW CRWNU XAYNP NNDIW ASDSV YPLLY EAIIS
 VYPOR FVSXO MPPNG RMWIO SHFJF TDQTW THSHK WOPEN SECWB UXCDT

DRUGS-7 van: Gompers aan: Schrevelaer

YOTBU DAPXS IFAXW YQRHI ECYSB JRZFI TMRMZ UOESK OSLVD VTOCN ANOOF
 WOTBJ OHRMZ VXOXF YQRHI ECEQA FVHEL IIIEH HDGDY ZMRCA DXBJZ ELWTJ
 FCIVV NNOOI VZCIH ZQKUV RVZBX AVZOP LYZLS GRBUL OBAVQ RXYNM LIBIZ
 FGMCG XEVMV ZZUHD UDIEU ERZRZ BKQGE VSLPS IFPEC OUQRN SOSJF IGIGT
 ACKRJ FOPMI IEHXY NMLIB IZFJR TKUGP ZSTQB MRLGR DMVTA AFOYA EVMIC
 EHHDB QBDMF IMZES IAPDZ ETTHZ SXQVE VSFWH AIVZT HWGKQ PXBRP ERMJR
 FCIYC QINMO REZXS XOOMU EFRTB QZQLE SSEFO DHVZS TMIUE VXPSQ RIOII
 OCFAR HERDS XUBZS EZIEB ECFMW HVHER UCUQB LHFBV EZLFA UTIKA RIAEK
 USHDE GMMV IQYXB ZZGBG GIQRB HJGIS AIDQH MWVZD UQDVZ RWCCX ARXII
 YOTBU ETOXN RZYLH FBXXX

DRUGS-8 van: Schrevelaer aan: Grote Baas

GAPLV RWJEC GXKMQ KPBHP XYUJO FBISO MPVXN IRPAK NIAOK EBUFK LEGWO
 UKQCB VYWGO MCVFA GBLEM MFSOB PTOSE NSONM DUSDA ZXXWR AMUXD HKLUS
 CUYCG IILDQ NCZSS NIJMO ZSLFS IXDBO EHLSF VMTYA XJVSP QHXAS LPXHS
 KQLPD DGPTX EBTPV WPYJD RRMVO FYIXK MEVFJ ZAQUW QVILV ASYYB KIMEB
 UVGAH MOVDC XGTNC QBQMW NFBHY SVNXC LLUAV HQBHH YDOHG XAJLR ZXLDZ
 IIDUV ZONYX PQFAK JLEBW JMECK NIAOK YBGSA HXBHX RRIDJ JDBAD UNXXI
 FAOJE WGXRW JSOBB OKVND ZMKIJ APXMR BZLWY UXPDE BDCXX

DRUGS-9 van: Doorzijker aan: Gompers

RZPEC OLGAE OAEWS HPGEL WLPEI YRENN DNNPV EBUDE NSEOB RNIEH ATAOT
KKEOC STORO GSETU GOIIO RRSOA WSUDR SMT00 EEETC ESVOZ

DRUGS-10 van: Doorzijker aan: Gompers

RZODP MTNIA PLAEP ENEOG ETSPE EEWD T WWRLP VGZUT PEU00 BRTNE EWECV
INKET KOHSE NLOEE TWGIR AEHEE GOWEL SEEAO TSAEE SUTCN GPITR ONERE
EWAER OZTEE SPGDT NMKXX

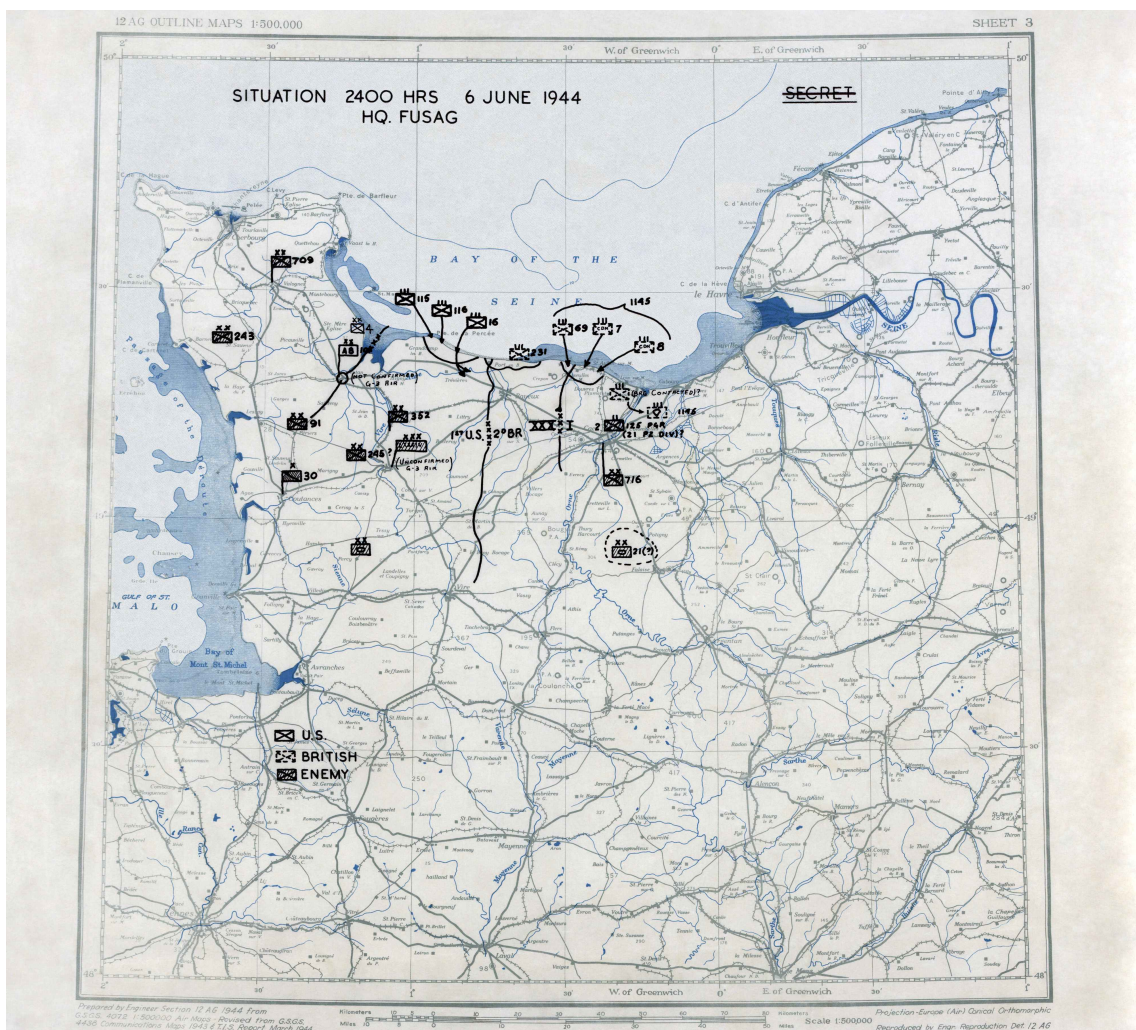
DRUGS-11 van: Doorzijker aan: Gompers

RZOTO EEETA RRRTE AEPTP EREOD SODRN PEAE ZATMK EEUAP VVBHN VLPPI
BRABR DMEIO THAED RCTKE TNTRN VSHOP ENGET ROIST NARAS HOEOW EGTIE
EEAVO NCREE SESEE TNTOP DEYON NRTOL EAJLE WTZTI RKHJI LDLTO NKXXX
NSOAE OESLN DSMMT MNDEG BOAOE AEOSA ETDDV MIONK BDDWN SKNJO EYRS
HCMNL OEEEE VCLOO PLEPK AOIAE TODRE MRLTE ILOPT ERITR TRNMN SOHAG
USXXX

9.3 Normandië oefening **

Inleiding

Enkele maanden voor de landingen in Normandië op D-Day (6 juni 1944) werd in Engeland een oefening in SIGINT gehouden (SIGINT = SIGnals INTelligence). De oefening speelt in de beginfase van de invasie, wanneer de invasiemacht nog betrekkelijk dicht bij de kust zit. De cursisten kregen in de loop van drie dagen zogenaamd afgeluisterde Duitse berichten in geheimschrift. Ze moesten deze ontcijferen en aan de hand ervan SITREP's schrijven (SITREP = SITuation REPort). Alhoewel de cursusleiders niet tot de kring van ingewijden behoorden, hadden ze toch als landingsgebied voor deze oefening de streek ten westen van Caen gekozen. Daardoor krijgen de berichten een zekere mate van authenticiteit. De onderhavige opgave is gebaseerd op de berichten van deze oefening.



Kaart van het landingsgebied

De figuur laat een kaart zien met de situatie op 6 juni 1944 aan het eind van de eerste invasiedag. De informatie over de posities van de tegenstander op deze kaart komt uit verkenningsmissies en informatie verkregen uit traffic analyse en cryptanalyse.

Cryptografische systemen

In de oefening maken we gebruik van twee verschillende cryptografische systemen, waarbij een van de twee in twee varianten voorkomt. Zodoende kunnen we elke aan het berichtenverkeer deelnemende Duitse legereenheid een eigen systeem geven.

De *305e Infanterie Division* gebruikt een variant op het Playfair-systeem. In de engelstalige literatuur wordt deze twosquare genoemd, in het Duits Doppelkasten.

De waarnemingsposten van de *29e Panzer Grenadier Division* laten we een monome-dinome systeem gebruiken. Dit systeem is op college behandeld en wordt hier niet verder uitgelegd.

De hogere regionen van de *29e Panzer Grenadier Division* gebruiken een vorm van Doppelkasten die in de Tweede Wereldoorlog ook werkelijk aan Duitse zijde in gebruik geweest is.

Het ligt voor de hand dat binnen elk systeem weer verschillende sleutels gebruikt zijn. We mogen er bij deze oefening van uitgaan dat elke eenheid een cryptoperiode van een etmaal in acht neemt, die om middernacht begint; sleutels worden dus gewisseld om 0000 uur. In zekere zin is dat genereus, want in werkelijkheid wisselde de sleutel vaker.

Eenvoudig Doppelkasten

We nemen twee vierkanten, het ene met het alfabet (minus de letter J) in normale volgorde en het andere gemengd d.m.v. een sleutelwoord. In het volgende voorbeeld is het woord TRAUMSPIEL als sleutel gebruikt.

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

De klare tekst wordt in digrammen vercijferd. Waar bij de Playfair de letters van het digram in hetzelfde vierkant staan, nemen we ze hier uit verschillende vierkanten.

Stel we willen in Doppelkasten digram FN vercijferen. Neem dan de F uit het vierkant links (1e kolom, 2e rij) en de N uit het vierkant rechts (3e kolom, 4e rij). Deze twee letters bepalen een rechthoek met als overstaande hoekpunten de Q in het linkervierkant (1e kolom, 4e rij) en de I in het rechtervierkant (3e kolom, 2e rij). Aldus wordt FN vercijferd tot QI.

Indien de letters op dezelfde rij staan, moeten we net als bij de Playfair de procedure aanpassen. We nemen dan de letters rechts van de te vercijferen letters, waarbij we de 1e kolom waar nodig op de 5e laten volgen. Dus LD wordt MF en LG wordt MB. Als de te vercijferen letters in eenzelfde kolom staan is er niets bijzonders aan de hand; AH wordt gewoon QT.

Merk tenslotte op dat het in Doppelkasten — in tegenstelling tot Playfair — niet nodig is om verdubbelde letters op te splitsen: RR wordt eenvoudig BK.

Voor de cryptanalyse kan men zich richten op de statistiek van digrammen. Waarschijnlijke woorden kunnen dienen voor het vinden van een deel van het rechthoek, dat op grond van de sleutelwoordconstructie vervolgens betrekkelijk eenvoudig kan worden gereconstrueerd. Verder valt gemakkelijk in te zien dat in vier op de vijf gevallen de relatie $PQ \leftrightarrow RS$ geldt.

Zonder dit sleutelwoord, d.w.z. met een volkomen willekeurige permutaties in het vierkant, is de reconstructie uiteraard lastiger. We mogen hierbij opmerken dat de Duitsers gewoonlijk het gebruik van sleutelwoorden vermeden. Beide vierkanten werden gevuld met een willekeurige permutatie van de letters.

Doppelkasten

In de bovenstaande, rechtstreekse vorm werd Doppelkasten door de Duitsers in de Tweede Wereldoorlog niet gebruikt. De klare tekst werd aan een — overigens zeer eenvoudige — transpositie onderworpen.

De codist schrijft de tekst uit in kolommen van zeg 17 letters breed. Als voorbeeld nemen we het bericht AN OBERGRUPPENFUEHRER VON DEM BACH, KIEW. BITTE DREITAUSEND SCHUSSPATRONEN SCHICKEN. De tekst begint dan als volgt:

ANXOBERGRUPPENFUE
HRERXVONXDEMXBACH
XKIEWSTOPBITTEXDR

...

De digrammen worden niet in volgorde van de tekst genomen, maar uit de overeenkomstige posities van opvolgende paren regels. Vercijferd wordt met de hierboven gegeven sleutel. De letterparen van het cryptogram staan boven en onder de respectievelijke digrammen van de klaartekst.

QCHDWZSRWPKEZOAPU
ANXOBERGRUPPENFUE
HRERXVONXDEMXBACH
TCYCATQINNFGACIKT

...

Het bericht wordt daarna digram voor digram uitgeschreven en in groepen gesplitst:

QTCCH YDCWA ZTSQR IWNPN KFEGZ AOCAI ...

Aan het eind van het bericht zal men òf tot twee complete regels moeten uitvullen òf de laatste twee regels in lengte aanpassen. Kan de lezer zelf bedenken waarom de eerste mogelijkheid minder gewenst is?

Voor de cryptanalyse dient men nu te bedenken dat de frequenties van de digrammen een andere is dan die in de taal zelf. De statistiek die we hier nodig hebben is die van willekeurig getrokken combinaties van letters waarbij voor elk van de letters van het paar de distributie die van de taal is. Het gebruik van X als woordscheider (zie onder) gecombineerd met het feit dat in het Duits de E een frequentie van tegen de 20% heeft, maakt de digrammen XX, EX en XE tot de meest voorkomende.

Opdracht en aanwijzingen

De formulering van de opdracht ligt voor de hand. Ontcijfer de berichten die door de genoemde Duitse strijdkrachten onderling zijn gewisseld op 1 en 2 april 1944, de dagen van de oefening, .

Berichten die binnen strijdkrachtonderdelen gewisseld worden geven in het algemeen geen mooi lopend proza te zien. Ze staan vol met afkortingen, jargon, code aanduidingen en andere eigenaardigheden. In deze oefening is daar niet al te veel gebruik van gemaakt, maar enkele komt men toch wel tegen. Hieronder volgt een overzicht van dit jargon.

Abt	= Abteilung	A = ANNA
Art	= Artillerie	B = BERTA
Aufklären	= verkennen	C = CLARA
Btl	= Bataljon	D = DORA
Div	= Division	E = EMIL
Batterie	= batterij (geschutsstelling)	F = FRANZ
Fla	= Flakgeschütz (luchtdoelgeschut)	G = GEORG
Fdl	= feindlich	H = HEIDI
Hptm	= Hauptmann (kapitein)	I = ILSE
Heeresrufzeichentafel	= call sign boek (stationsroepnamen)	J = JOHAN
Gefechtstand	= commandopost	K = KLAUS
Kdr	= Kommandeur (commandant vd eenheid)	L = LUISE
Kettenfahrzeug	= rupsbandvoertuig	M = MAX
Kfz	= Kraftfahrzeug (motorvoertuig)	N = NINA
Komp	= Kompanie (compagnie)	O = OTTO
Lagebericht	= sitrep (begin/eind vd dag)	P = PETER
Lt	= Leutnant (luitenant)	Q = QUIRIN
Melder	= ordonnans	R = RUDI
Pak	= Panzerabwehrkanone (antitankgeschut)	S = STEFAN
Panzer Grenadier Div	= mobiele infanterie divisie	T = THEO
Pz	= Panzer (tank)	U = ULRICH
Pzkw	= Panzerkraftwagen (tank)	V = VICKY
Off	= Offizier	W = WALTER
Oblt	= Oberleutnant	X = XANDER
Oberst	= kolonel	Y = YSER
OP	= Observation Post	Z = ZENO
Regt	= Regiment	
Roem	= Römisch (romeins cijfer volgt)	
Sanka	= Sanitätswagen (ziekenauto)	
Sfl	= Selbstfahrend (gemotoriseerd geschut)	
Spähtrupp	= verkenningspatrouille	
Uffz	= Unteroffizier	
Zug	= afdeling	

Afkortingen en spellingsalfabet

1. Een van de dingen die een bericht lastig te lezen kan maken is het ontbreken van woordscheidingen. Nu zit de ontvanger van het bericht met datzelfde probleem en wat meer is, hij zou daardoor fouten kunnen maken met wellicht desastreuze gevolgen. Daarom ziet men vaak de woorden op een speciale manier van elkaar gescheiden. De Duitsers gebruikten daarvoor als regel de X. Zodat DER MANN in een bericht verwerkt wordt als XDERXMANNX; de X'en scheiden de woorden van de elkaar en van de

omringende woorden. Merk op dat de X hierdoor een hoge frequentie krijgt en daarmee een goed aanvalspunt voor de cryptanalyse vormt.

2. In de praktijk heeft de cryptanalist geregeld te maken met onvolledige of gebrekkige berichten. Fouten kunnen op diverse plaatsen optreden: bij het coderen zelf, bij het overseinen en bij het opnemen van het bericht. Vaak ook heeft de opnemer delen van het bericht niet kunnen horen door ongunstige ontvangstcondities veroorzaakt door atmosferische storingen of doordat het af luisterstation ver van de zendende partijen gelegen is. We maken de oefening niet moeilijker dan nodig, d.w.z. de cryptogrammen zijn zo foutloos mogelijk.
3. Plaatsnamen en eigennamen zijn natuurlijk bijzonder belangrijk in berichten en daarom worden deze voor de zekerheid herhaald. Bovendien worden er veelal nog J's omheen gezet om begin en eind van de naam duidelijk te laten uitkomen. Een voorbeeld, de plaatsnaam Caen wordt opgenomen in de vorm JCAENJCAENJ. Als het systeem geen J bevat (zoals in systemen gebaseerd op een 5×5 vierkant) kan hiervoor weer de X benut worden.
4. Belangrijke woorden kunnen worden herhaald. Zoals AN (Duits an = aan) waarna de geadresseerde volgt, en VON afzender. In het bericht vindt men dan ANAN en VONVON.
5. De Duitsers wisten natuurlijk ook wel dat de CH (in het bijzonder in SCH) een kenmerkende combinatie vormt. Daarom verving men deze vaak door een Q; b.v. NAQT voor NACHT.
6. Berichten worden nooit zonder meer verzonden, maar altijd ten behoeve van het berichtenverkeer voorzien van zaken als: afzender, geadresseerde, volgnummer, tijd en datumgroepen, authenticator, voorrangstekens, enz. Het analyseren van deze toegevoegde informatie vormt de basis van de zogenaamde TA of Traffic Analyse. De Nederlandse uitdrukking hiervoor is berichtenverkeersanalyse. Uit TA kunnen belangwekkende inlichtingen worden verkregen, zelfs al kan men de inhoud van de berichten niet lezen. Anderzijds levert TA ook vaak nuttige aanwijzingen ten behoeve van de cryptanalyse. Een voorbeeld van zulke voorrangstekens zijn de groep SSD = sehr sehr dringend en KR of KRKR = Ich habe ein Kriegstelegram. Alle op dat moment op dezelfde frequentie werkende stations moeten dan zwijgen om het belangrijke bericht niet te storen. In deze oefening laten we dit aspect weg.
7. De berichten van de 305e Infanterie Divisie (in eenvoudig Doppelkasten) vertonen in het linkervierkant de normale lettervolgorde (zonder J) en in het rechtervierkant een sleutelwoord.

De berichten van de 29e PGD (in Doppelkasten) gebruiken een vaste lengte van 17 letters per regel, een linkervierkant in de normale lettervolgorde (zonder J) en een willekeurige permutatie in het rechtervierkant.

Merk op dat in de Tweede Wereldoorlog de cryptanalisten te maken kregen met steeds wisselende regellengte en twee willekeurig gevulde vierkanten, terwijl deze sleutel ook nog eens om de 8 uur wisselde. Om een idee te geven van de benodigde hoeveelheid materiaal voor analyse: Poolse cryptanalisten uit de Tweede Wereldoorlog

hadden berichten in eenzelfde sleutel met tezamen circa 2000 letters nodig om tot een oplossing te komen; daarbij dienden genoeg herhalingen voor te komen om de (wisselende) lengte van de regels te kunnen bepalen.

8. Het gebruikte spellingsalfabet alsmede speciale afkortingen en uitdrukkingen staan in de bijgaande tabel. Let op! Er zijn vast wel speciale uitdrukkingen die aan het begin van een bericht kunnen voorkomen of die een herkenbaar patroon van letterherhalingen vertonen. Indien herkend, dan kunnen deze uitdrukkingen de analyse flink op weg helpen.

Cryptogrammen

NORMANDIE-1 1 april 1944 - 0500 uur : 29 Panzer Gren. Div.

van: waarnemingspost

aan: 2e bataljon

39565 83236 85339 36373 45283 25933 34375 33138 44365 82365 39735
39536 52363 43038 52345 82365 23038 52345 82365 23059 90593 33437
53313 84436 58236 53903 53965 38565 83453 64583 86636 83558 36521
53737 38583 85339 38535 39831 36584 38599 85933 34375 33138 44365
82365 39496 96393 64365 85385 65834 51366 43064 59573 85237 53345
25354 36588 38553 06459 57385 23753 34525 35436 58838 55305 93236
63839 45354 36586 70526 65398 93969 65138 36058 36834 53343 65853
83850 45337 36310 38334 36853 54365 83536 05853 35364 43683 33805
81365 23236 53385 23353 64583 86636 30423 73755 30423 73755 30645
82703 03138 37373 65856 55303 13837 37365 85655 30593 74596 70563
68363 93888

NORMANDIE-2 1 april 1944 - 0700 uur : 29 Panzer Gren. Div.

van: 1e bataljon

aan: regiment

BOMRD BNDNA YWOKY HLRFA MAAQS ENFCQ LROLI YSDTC ZTKWU CSDOI KBAXM
XXXZO DRIWX KSXDK NNWIK QAETP ZQOIH ZPRSC VVPAA EMWXX

NORMANDIE-3 1 april 1944 - 0712 uur : 29 Panzer Gren. Div.

van: regiment

aan: 2e bataljon

NKICL RSIYO LAZKO IFSOL CNNKP ELSYE MBDYU CTCNB YKLTH AYTYZ MTKOB
LDBVO NFCBO BPTFG OSSIY VKQYD LEPKX IFWDB SZWAP KHGOS SDYTA QMBNZ
BOXXX

NORMANDIE-4 1 april 1944 - 0800 uur : 305 Inf.Div.

van: 576e regiment

aan: divisie hoofdkwartier

FDMHM IBPHI YRZDO LYROC NXVGL HNUUT HWFZC BSYHI GUHIC WOTYW TLCRT
MXRBP HIYOC DSYIO KRKBS YIOKR KBCYQ SPPNF MHRUB QKFSV KQEBN UMPYB
MHGHC DKFZT ZDOLY RNPDB HWPRV LNPHI XRXDM MHWPR VLGGI BSAVB TGZPM
PXRTG ZPMPX RKBNV DAKFU THVFF YTXXX

NORMANDIE-5 1 april 1944 - 0810 uur : 305 Inf.Div.

van: 577e regiment

aan: divisie

FDMHM IBPHI YRCRT ENVKB HOFGA VUTFG VIOHW RAVUT SVKQE BNWAF OKCWO
TCXLI DPMNA FYRGU KIMPO ENUUT HWQFY RC RTE

NORMANDIE-6 1 april 1944 - 0812 uur : 29 Panzer Gren. Div.

van: 2e bataljon

aan: regiment

NCOKB RHAYT UXEKO IPMOB YHNAU PVAEO KBCXB QOXOR YDXLO BBQGX IRDXB
LDCHD PLOAA FPTMP BQOYU KPRMK TVAPY DOEBQ NQSUN FMIII OASCM APTMS
POXXH FMTKO MLOBB QYFNB YYZTM IWQLR PKPRM LXXIU IILVN FBQZC GVNFN
VPIUO LOMWZ OCDDQ MXBRG YVTSN BXQRN FCFEN MHPTC BPYZT VIMIK TNH UD
WZPTO SNDXX IEBCI QYDUV DLWVP CAQOX QUNFP WRICL YDMZA QNYUK NFXXX

NORMANDIE-7 1 april 1944 - 0830 uur : 29 Panzer Gren. Div.

van: 1e bataljon

aan: alle stations

NIKYX XYVNN WIAQM AOKB CXBVC ZUFMH AODWA OMKOU ZTOXY DNKPX QSDXM
KXXXX

NORMANDIE-8 1 april 1944 - 0900 uur : 305 Inf.Div.

van: divisie

aan: 576e regiment

PAWRT TAFHW PRCWP PCKNU YHYXT BYTMI YBMPB BNVKB XRVXY LXDMM HWPRV
LFFUA NDKFS YUSKA XBPBA FHDZR

NORMANDIE-9 1 april 1944 - 0905 uur : 29 Panzer Gren. Div.

van: waarnemingspost

aan: 2e bataljon

38863 83939 37528 32533 33437 53353 85836 44368 53528 34536 59335
93759 28535 13837 34533 13625 33158 52367 35365 37373 85838 53393
85353 90313 65843 85364 56575 36705 63683 63938 88000

NORMANDIE-10 1 april 1944 - 0950 uur : 29 Panzer Gren. Div.

van: 5e compagnie

aan: 2e batterij

LSZQD WOIIIO NDPSD ENIUX FPOIY WAPCF XLDLC KOBCF MOLRO KXXXX

NORMANDIE-11 1 april 1944 - 1100 uur : 29 Panzer Gren. Div.

van: 6e compagnie

aan: 2e batterij

XHBOC EHACZ AMMIQ RNFES LRNGE XXXXX

NORMANDIE-12 1 april 1944 - 1115 uur : 29 Panzer Gren. Div.

van: 2e batterij

aan: 6e compagnie

OTSLP QKSCZ ZBCXE QHHAZ DMPTM BNDVW FEVPG HZQDS LNOVZ TMKGS PYAQH

NORMANDIE-13 1 april 1944 - 1120 uur : 29 Panzer Gren. Div.

van: 3e batterij

aan: 9e compagnie

AWPKP QXWMK AQMBN ZNLIG LSYXB KXXXX

NORMANDIE-14 1 april 1944 - 1200 uur : 29 Panzer Gren. Div.

van: regiment

aan: 3e batterij

OTGYZ TDWNF EEFRE WNFRO QODKI BAUBL DMPTP NRFPQ DWCPN BCEOO NFWDO
WZPGK NFLGB OPSMB CFFRC OOBSD QCCXO KXXXX

NORMANDIE-15 1 april 1944 - 1700 uur : 305 Inf.Div.

van: divisie

aan: 576e regiment

MPBHN KCLCW PPCKS YOHMI XLCPK TKFSY POTMY RGDYY MIBRV TTTAF NUMPY
BXDMM HVZGO PHUCI PTPKC RNUQS VRMPB BCWPP CKHUH IYRCP KTKFC RTEXX

NORMANDIE-16 1 april 1944 - 1810 uur : 29 Panzer Gren. Div.

van: 2e batterij

aan: regiment

LVZTO WHIEP AEKSL YAQHF UGVQO IKDAP WKNNN WIEIY OBYII KNFIU DXIBD
KIDIC NNCGL QRLNZ NBZEF QPRYY CFENP KXXXX

NORMANDIE-17 1 april 1944 - 1830 uur : 29 Panzer Gren. Div.

van: 2e batterij

aan: regiment

NKUYP QAXAX PBCEM VNFWD PIHAN FQFOS AQBBP XVXVG OBCFL IKLOA ESYKN
DETBK PRDWN NEGKB CXPSO KHFUP YUHPV RCEPT YHFHP RWKVE EKPRY ZCPFR
DKOKZ OGYDS ATNNW FPAXA YDNKE CLTCG KHZTS LCNLT CGMUZ TWMMB DSLUV
WPPCE YWQWA WNNLR MOMMP RXDOS PTHLP RCESD KAKBO BKRHF NGLPX

NORMANDIE-18 1 april 1944 - 1835 uur : 29 Panzer Gren. Div.

van: 1e batterij

aan: regiment

PTIBR ZVQHH LFDWZ PMBXX PKFEM ACEKC MAVXD CPIOY YDXBA QMYNE PROII
KDIOK NZNBY BPADO NUYKX LXXXX

NORMANDIE-19 1 april 1944 - 1920 uur : 29 Panzer Gren. Div.

van: regiment

aan: alle stations

WTKRV WKQSV QINKR XLOUO CLHCO SBWNF AQQWM ZPRSY ORZTO IHBDX AVDGM
KUYNF FRCRB SPRSO XWKYS IRVNN UFMFP OOWXI PLFIM IHEEK MXMTN HFQZK
OXQQO NXXXX

NORMANDIE-20 2 april 1944 - 0800 uur : 29 Panzer Gren. Div.

van: 1e batterij

aan: regiment

BQTGB UREKV XDNCG ZAOFN OWQPC NWBYI HKYPK YRMEF PXYEY UYAXC BOKOS
FMUZW CNISH AEXUR LXXGI VSHES KKMPA PCCRG UXMQT VZSWK SIANK XHARX
FVUKI PKVSK KYZWX GXXXX

NORMANDIE-21 2 april 1944 - 0815 uur : 29 Panzer Gren. Div.

van: 2e batterij

aan: regiment

LXANF NKVSC GVQOI PIKUO GKYYZ SXXXX

NORMANDIE-22 2 april 1944 - 0835 uur : 29 Panzer Gren. Div.

van: 4e batterij

aan: regiment

FGFVR MKVWD ZSANE XKKXD WBCCL FUXQP UWBPY BZSWW KVHNH NQPVD FZONK
KQQAN ZZPUO NUMTF GYLFH CCNEK FZQQQ XSOCB YKZXY MXGHK AFFAU OBUQN
PUNLD UKOYI VSHZS HWDVV UWSGS NHZEF YKUCB TPSKY HCWEU WTPHV NFEUP
VIKVA XDOUA OCHGX FXDUI KZWMU DFUXH CIUPD DUKXK KZSCN LECIG ZWCN
SNHCF CPVBU GCQRH ZOXLE UCAXX EHQQH GZLXH GSQSC XNZOB ULIUO HZOFN
QBOXX

NORMANDIE-23 2 april 1944 - 0900 uur : 29 Panzer Gren. Div.

van: 4e batterij

aan: regiment

NDKKX QOFYP KYDNH GYIWS ZSHKU KVWHZ EOYID ONEDL HAZDE UCZZY IKSHB
OHXSF IKNCH XBNHK SOCFE KXLHK SHECP TSHKV OFXZX PHALC DFVYE UZXHQ
AFHAV TMCAX DFCAY WKASH ECMCK VEUCZ YTGVS KBOCG IVXUZ QEPBU HAVTM
CAXDF NLUQG KZWCN RBNAE OSLAV TBHCE OMPUO DFCTI KDNZZ YHZOV GAFUU
UXNCR VVSDU YKZXW RYBHT HVNQC COVMK AOOEC IKVOF CNXKY HXRYB AOEGE
CHAWY MUCTE CMIPV DFHAX WNQCT AOOEC DPXOB CCLIT MKVWL CCPIR HKVYY
CCNLU QGKZW NAEDE HHAUY INZGG YCCHF WKYCX PIKTQ ZDHAN CECGC UXKYN
CHXBN NCQCT YUWBU CTSGU OKKCN MFSCU WTYCN HPSHW IOFPW PPSTQ CTMAO
BKTYA OSUNA CNUVE RSGHC CNPSQ KCNCT XGERQ GXXXX

NORMANDIE-24 2 april 1944 - 0920 uur : 29 Panzer Gren. Div.

van: 11e batterij

aan: regiment

VSXZB OSGHA TODBA HNCLC KYUWB UNIRO KWLK CPESR LSXZP FPSXX

NORMANDIE-25 2 april 1944 - 0930 uur : 29 Panzer Gren. Div.

van: waarnemingspost

aan: alle stations

60176 03035 45301 59069 57540 68265 85958 20653 01570 67954 06560
10602 65457 06158 56061 25358 51505 80651 54626 06036 06471 58286
78307 70835 80158 03601 01000

NORMANDIE-26 2 april 1944 - 1000 uur : 29 Panzer Gren. Div.

van: 4e bataljon

aan: regiment

QNQWR YAOGS ZVWPY BHVSM YLHAA OTEHZ XLOQK VYTWB AOGYZ WNXCB IKXLO
UBXAO IPYEW BZBHC AFTVQ NSHOE BOPXW EZXWR BOXGW EMPKY ABWVG PPPFK
CTVHX AAVDB CTKYL XAOHY ZWMUC CRYUW HKNXC FKKZW OUECS CFXKU NKBFP
WQMFV KYYTN QBXOD CDHAW TAOGP XIZPX GEUV IKYTX GYIHY ZSVYP SSVIY
YLXPX

NORMANDIE-27 2 april 1944 - 1055 uur : 29 Panzer Gren. Div.

van: waarnemingspost

aan: 2e bataljon

60176 03035 45301 59065 30306 41434 84309 30106 58565 95801 58010
61303 15820 10603 56806 59538 58206 02562 50530 15906 60159 58592
56995 80104 58560 10658 56595 80158 70695 45359 00585 35906 52560
18582 06575 82069 23018 06615 95875 15237 75801 06783 07756 58075
85400

NORMANDIE-28 2 april 1944 - 1330 uur : 29 Panzer Gren. Div.

van: 4e compagnie

aan: 2e bataljon

UWTYC NHPYT ETBCK VYYNC ATDFP WSKHA XDEUH NZPFZ ANNAC DKKVD VGHAC
OZSUB BOZVW NZQOU NIENP ACIHK ZDBOU SNERA BSBFP VCDHA ZLSHZ EGDHA
CNTDB ROXMT UOXKI LHAAN DGXGB MKZPC BCAST FSHLG KANCC UKGFV AXNMX
IFVMY OFMYD UNCZK XNYOC COXAV SKNIA IKVBP WSBOP VWWMB KVOXG KBOAW
HZRMU PUNEP XGFYD UYCDN IRYIP XOFCN CKHAQ KAYQF PCNII VWPAO KYDFH
ZXLNC DGAFL ECIKV YYCNH RYIPU LFAFE CXXXX

NORMANDIE-29 2 april 1944 - 1700 uur : 29 Panzer Gren. Div.

van: 2e bataljon

aan: 4e compagnie

ABZPA VSUCC YQGVQ QOKSI CNPSQ PSFFV ZUTLB CKPKV HNCRS ONYKV SHQXP
ULBCC OESFG RAOTQ ROFZU KCUDR IKGZU QABVS

NORMANDIE-30 2 april 1944 - 1800 uur : 29 Panzer Gren. Div.

van: 7e compagnie

aan: 3e bataljon

CODBY PUKZW NHCUY GAMPQ MUIKC CLSHV CBYUC FLXZV LMDUH PVIYB WGGZU
OWLGA BOBBZ XXQKY NXEFX

NORMANDIE-31 2 april 1944 - 1815 uur : 29 Panzer Gren. Div.

van: 3e bataljon

aan: 7e compagnie

EUCZB QTQPV RFMDY YFKYA IVLXC UNIWE ECGAG UHUDU UVOQX KSTRS AOIUS
RKYUO COXKI PYGSI SDEUS PYTVC GAUOD FNACD KKVDV GHAQ EPHAZ FUVTF
OQPSC TIRBV GKONS IZLOZ TVHAY WOUAO XZSIE XBUKY YLOUP VXDNP HABCL
WHYUO HACPY UVOCV NUWSB OUROU NIBNP LTRTK UHWMS AQFPX OBCNT XMQOY
DOIEA VYCEH QKBCD BWUIY QOOWK VOQCC BEZWH KRKZP KVDPE CIKCT BCTYX
LYUYA BNDYG KYTXG KYRKD UHHWZ PQPXB FTOEU SRNXN YCCPS HKHUZ VHZDP
BPFVU OBFVP ZLNCF AAOMP HKINW KHYAX CGHAT OBOHT FYAXH VNFLX GYLFA
OHNSC GAPXG UYSKV CGCCF YDGCC DEHKU KSAKK XQRQD NKOWY VGDF A PCHTY
WNNFC CASYE ONHAP UCNME UXDUK UZVXQ SHFAP QNTEN ZLCGZ BDUSA GVZWO
FCCFV QKCPW EVSOD CTWGD MSUCC EIKKY CZSWL XHVOB UDUAO CNCCX

NORMANDIE-32 2 april 1944 - 1830 uur : 29 Panzer Gren. Div.

van: 7e compagnie

aan: 3e bataljon

VSCNV WHQCC MAKVU PDUKY XWNFC TKZZL OQEBL YKKZS CNABY TLZBO SLDMX
UYACO UVAMK ESGVZ ZXYRD PKVCN HCQRH ZTOCC WIYNW RYSAO WPDQS GCNAS
HAPIH YUYGH YINUO UXXXX

NORMANDIE-33 2 april 1944 - 1840 uur : 29 Panzer Gren. Div.

van: 7e compagnie

aan: 3e bataljon

WVPSG YPXCF AZCHT OPVTR NAZYI VWRHK NCBCZ DZUXQ EFOPY TKSYP CNHAE
PCNNQ YDZXW MVGXX

NORMANDIE-34 2 april 1944 - 1855 uur : 29 Panzer Gren. Div.

van: 3e bataljon

aan: 7e compagnie

RHLXB FZVHG NTHZF XXVXM SHFAP QXXXX

NORMANDIE-35 2 april 1944 - 2035 uur : 29 Panzer Gren. Div.

van: 3e bataljon

aan: 7e compagnie

FAPXB UVYMQ EUSXN FIUZV UPUWB UYIRC FXBFG VMLER AXXSE FZXYI ZOYVO
NNCFY BGCCX UZKXB VSHYC NAXXP UQZKC GEBIK PFDZG ZUQAG ZSTQE NVBER
XGBFC TZGER SGEFY RQBVS IEBUA SVOIK UKXXX

9.4 Pearl Harbour oefening ***

Inleiding

In de vroege morgen van 7 december 1941, verschenen onverwachts Japanse vliegtuigen boven de haven van Pearl Harbor op Hawaii en vernietigden een belangrijk deel van de Amerikaanse vloot in de Stille Zuidzee. Deze oefening is gebaseerd op het Japanse berichtenverkeer voorafgaand aan die actie.

De directe opdracht voor de oefening is het reconstrueren van de sleutel(s) tot een reeks berichten, die in de aanloop tot Pearl Harbor binnen de Japanse zeestrijdkrachten zijn gewisseld. Deze berichten zijn na afloop van de Tweede Wereldoorlog gedecodeerd en sommigen beweren dat tijdige ontcijfering ervan de Amerikanen voor de aanval had kunnen waarschuwen.

Cryptografisch systeem

In de periode voor de aanval op Pearl Harbor maakte de Japanse Marine gebruik van de zogenaamde J19-K10 gecombineerde code. J19 is een tweedelige code, K10 een kolomtranspositie met complicaties. Een bericht werd eerst omgezet in code, waarna dit gecodeerde bericht aan de kolomtranspositie werd onderworpen.

Als voorbeeld van dit systeem geven we een bericht dat eveneens een belangrijke rol gespeeld heeft in deze periode, nl. de zogenaamde 'winden'-code. Dit was wat men noemt een 'open code', een onschuldig klinkende tekst met een speciale betekenis. Ze was bedoeld om in het geval van onmiddellijk dreigende vijandelijkheden de Japanse gezant in Washington te kunnen waarschuwen.

De code ontleent haar naam aan de dekmantel waaronder deze waarschuwing ging, nl. een weerbericht. Met „oostenwind regen”, „noordenwind bewolkt” en „westenwind helder” werd geduid op aanstaande vijandelijkheden tegen respectievelijk de Verenigde Staten, de Sovjet Unie en Zuidoost Azië (Thailand, Malakka, Nederlands Oost Indië). We geven eerst de tekst van het bericht in Nederlandse vertaling.

Betreffende het uitzenden van een speciaal bericht in een crisissituatie

In een crisissituatie (gevaar voor het afbreken van onze diplomatieke betrekkingen en afsnijden van de internationale communicatielijnen) zal de volgende waarschuwing worden toegevoegd in het midden van het dagelijkse nieuwsbericht in de Japanse taal op de korte golf.

1. In het geval de betrekkingen Japan-US in gevaar zijn: *HIGASHI NO KAZE AME*.
2. Japan-USSR betrekkingen: *KITA NO KAZE KUMORI*.
3. Japan-Groot Brittannië betrekkingen (inclusief Thailand, Malakka en Nederlands Oost Indië): *NISHI NO KAZE HARE*.

Dit signaal zal worden gegeven in het midden en aan het eind als een weerbericht en elke zin zal tweemaal worden herhaald. Wanneer dit wordt gehoord dienen alle codeboeken, e.d. te worden vernietigd. Voor het moment is dit een zeer geheim arrangement.

Doorgeven als dringende informatie.

In de figuur staat de met J19 gecodeerde Japanse tekst van dit bericht.

Kancho fugo	atsukai	Kokusai	jigyo	no	hip	pa	ku	no	kekka	itsu	saiaku	no
XEIC	NC	ST	WYNY	KY	ES	NI	CU	KY	MTAN	WEUF	DB TH	ZW
jitai	ni	tachi	itaru	kamo	hakararezaru	tokoro	kakaru	baai	waga ho	to	aitekoku	
JXHZ	US	GKIY	IO	WV	MTGS	WU	YK	UQEQ	XF	UX	KZRS	LJ
to no	tsushin	wa	tadachi	ni	teishi	serarubeki	wo	waga ho	no	gaiko	kankei	
SC	FW	AO	AD	CE	CY	SI LW	BS BN	FK	XF	ZW	LUGS	XEYM
kiken	ni	hinsuru	baai	ni wa	waga	kaigai	hoso	no	kakuchi	muke	nihoho	news
LZFF	US	TR GD	UQEQ	XG	FH	EK FG	XJKC	KY	PE IY	ZTVE	FJ FX	VAIX
no	chukan	oyobi	saigo	ni	oite	tenki	yoho	to shite	1	.	Nichibei	kankei
ZW	MS	ZP	KR	DB	NX	AE	NE LZ	LJXJ	CT	NC	LA BO	TMWD
no	baai	ni wa	"	higashi	no	kaze	ame	"	2	.	Nichiso	kankei
KY	UQEQ	XG	HL	CUOM	LW	KY	FEXD	DWLD	VB	NC	JG BO	EF PB
												XEYM
baai	ni wa	"	kita	no	kaze	kumori	"	3	.	Nichiei	kankei	no
UQEQ	XG	HL	VM	KY	FEXD	CUCN	JM	VB	NC	TK	BO	OCXP
												XEYM
(	"	shinchu	mare	"	Netherlands East Indies	koryoku	oboe	fukumu	"	"		
WM	HL	AO MS	MD QC	VB	MTOV	ER	CX	NV	FAXP	ZT	VB	HL
nishi	no	kaze	hare	"	o	2	do	zutsu	kurikaeshi	hoso	sessimeru	
ZA	LW	KY	FEXD	KPQV	VB	NC	NV	JG	UP	QOAF	UF	XEEQ
												XJKC
												GG
koto	to	seru	wo motte	migi	ni yori	ango	.	Shorui	to	tekito	shobun	aritashi
BV	UX	NJ	FX	DM	MG	RA	VD	BO	AD	BE	RV	TMKD
												AD JB
												GQ NC
Nao	migi	wa	gen	ni	gokuhi	atsukai	to	seraretashi				
NU	DM	AG	VP	US	BDZK	?B	UX	ZH				

Klaartekst winden-code

De gecodeerde tekst wordt vervolgens in het transpositieblok van de K10 kolomtranspositie geplaatst (zie de figuur). De permutatiesleutel heeft hier lengte 19. Wat verder opvalt zijn de zwarte blokjes, die voornamelijk in de bovenste rijen voorkomen. Deze blokjes geven aan dat de betreffende positie niet met een letter mag worden gevuld en dus wordt overgeslagen. Hierdoor krijgen de kolommen een verschillende lengte, waardoor de reconstructie van het transpositieblok wordt bemoeilijkt.

Vervolgens worden de kolommen in volgorde van de sleutel uit het transpositieblok genomen en verdeeld in groepen van vijf letters. Als het bericht lang is, wordt het in meerdere delen gesplitst. Deze delen worden voorzien van afzender, geadresseerde en enige verdere aanduidingen zoals systeemindicatie, voorrangscodering, authenticator, e.d. Weergegeven is zo'n telegram in de vorm waarin het door de Amerikaanse af luisterdienst werd onderschept; de cijfertekst is in twee delen gesplitst.

Opdracht en aanwijzingen

Er volgt nu een serie berichten uit de maanden september tot en met december 1941. Deze berichten hebben betrekking op de voorbereiding tot de aanval op Pearl Harbor. Zoals

3	17	12	4	5	18	2	10	19	7	11	9	14	1	6	16	13	15	8
X	■	■	■	■	■	E	I	C	■	■	■	■	N	■	■	■	C	S
T	■	■	■	■	■	W	Y	N	■	Y	K	Y	E	■	S	N	I	C
U	■	■	■	■	■	K	Y	M	■	T	A	N	W	E	U	F	D	B
T	■	H	Z	■	■	W	■	■	■	J	X	H	Z	U	S	G	K	I
Y	■	I	O	■	■	W	V	M	T	G	S	W	U	Y	K	U	Q	E
Q	X	F	U	X	■	K	Z	R	S	K	H	S	C	F	W	A	O	A
D	C	E	C	Y	■	S	I	L	W	B	S	B	N	F	K	X	F	Z
W	L	U	G	S	■	X	E	Y	M	L	Z	F	F	U	S	T	R	G
D	U	Q	E	Q	X	G	F	H	E	K	F	G	X	J	K	C	K	Y
P	E	I	Y	Z	T	V	E	F	J	N	X	V	A	I	X	Z	W	M
S	Z	P	K	R	D	B	N	X	A	E	N	E	L	Z	L	J	X	J
C	T	N	C	L	A	B	O	T	M	W	D	X	E	Y	M	K	Y	U
Q	E	Q	X	G	H	L	G	U	O	M	L	W	K	Y	F	E	X	U
D	W	L	D	V	B	N	C	J	G	B	O	E	F	P	B	X	E	Y
M	Z	W	U	Q	E	Q	X	G	H	L	V	M	K	Y	F	E	X	D
C	U	C	N	J	N	N	B	N	C	T	K	B	O	O	C	X	P	X
E	Y	M	K	Y	U	Q	E	Q	W	M	H	L	H	Z	V	B	A	O
M	S	B	L	M	D	Q	V	M	O	V	B	M	T	O	V	E	R	C
X	N	V	F	A	X	P	Z	T	V	B	H	L	Z	A	L	W	K	Y
F	E	X	D	K	P	Q	V	V	B	N	C	N	V	J	G	N	P	Q
O	A	F	U	F	X	E	E	Q	X	J	K	C	G	G	B	V	U	X
N	J	F	X	D	M	M	G	R	A	V	D	B	O	A	D	B	E	R
V	T	M	K	D	A	D	J	B	G	Q	N	C	N	U	D	M	A	G
V	P	U	S	B	D	Z	K	?	B	U	X	Z	H	M				

Vercijfering winden-code

SF DE JAB 8 NOV 41

361 SCDE TOKIO 90 19 9 40S JG P1/50 3805

RIYOJI SANFRANCISCO

MWZHU BUWTJ NEWZU CNFXA LEKFK OHTZV GONHE WKWWK SXGVB BLNQV

QQPQE MDZXT UTYQD WDPSC QDMCE MXFON VVZOU CGEYK CXDUN KLFDU

XKSXY SQZRL GVQJY MAKFD DBEUY FFUJI ZYYPY OZOAJ GAUMT SWMEJ

AMOGH CWOVB XAGBS CBIEA ZGYMJ UDYDX OCYQX RKGAX SHSZF XNDLO

VKHBH CKDNX IYYVZ IEFEN OGCXB EVZVE GJKYT JGKBL

1320 S RJ

9160

F DE JAB 8 NOV 41

P2/360 41W KOS WASHN 3804

KNEWM BLTMV BNJVQ UHIFE UQIPN QLWCM BVXFF MUNFG UAXTC ZJKEX

EXBEW UVBMY NHWSB FGVEX WEMBL MLNCB CZCID KQOFR KWXYS EXPAR

KPUEA SUSKW KSKXL MFBFC VVLGB DDXCL UEZTE WZUYS NEAJT PXDTA

HBENU DXPXM ADCNM MRLYH FXTUJ GNQMT VQRB 84444 BDSHD TAKAO

TOGO

(VQRB) AS SENT

1317 S RJ

9160

Tweedelig cryptogram winden-code

men ziet zijn ze uit verschillende delen van de Japanse strijdkrachten afkomstig. Deze berichten zijn met een vereenvoudigde J19-K10 gecijferd en moeten worden opgelost. Er zijn enkele aanwijzingen die kunnen helpen om de sleutels van deze cryptogrammen te breken. In willekeurige volgorde geplaatst luiden deze:

- De taal van de klaartekst is Engels.
- Een kolomtranspositie kan het gemakkelijkst worden opgelost, wanneer twee berichten met eenzelfde beginstuk of eenzelfde eindstuk worden gevonden. Het is dan betrekkelijk eenvoudig om de indeling in kolommen terug te vinden. Hieruit volgt het aantal kolommen en, in het geval van de K10, ook een aanwijzing voor de plaats van de uitgeblokte roosterposities.
- In deze opgave zijn de systemen J19 en K10 wat vereenvoudigd. De transpositie vertoont in de afgeblokte posities wel ongeveer het beeld zoals in het 'winden'-bericht, maar er is toch een vereenvoudiging op aangebracht. De substitutie is geen compleet codeboek zoals J19, maar een betrekkelijk eenvoudig digramstelsel: voor een letterpaar (een rij- en een kolomcoördinaat) wordt in een vierkant of rechthoekig rooster een substituent gegeven.
- Het berichtenverkeer omvat verscheidene cryptoperioden, d.w.z. tijdvakken met een verschillende sleutel. Echter in een lopend communicatiesysteem wordt in opeenvolgende cryptoperioden nogal eens gewerkt met variaties op een vorige sleutel, gedeeltelijke veranderingen in de sleutel, e.d.
- Alle berichten bevatten een veelvoud van vijf letters. Dat kan geen toeval zijn.
- Medewerkers van de codekamer maken wel eens fouten. Vaak levert dat berichten op die het breken van de sleutel geweldig vergemakkelijken. Ook in deze serie is zo'n fout gemaakt; spoor die op door alle berichten goed te bekijken. Vandaaruit kan stap voor stap de berichtenserie worden gebroken.
- Uit andere bron is men te weten gekomen dat het codewoord voor de aanval luidt CLIMB NIITAKAYAMA. De symboliek van deze code met betrekking tot de aanval op Pearl Harbor is duidelijk: de Niitaka is de hoogste berg van Japan.

Cryptogrammen

PEARLHARBOR-1 September 5, 1941

van: Chief of Staff, Second Fleet

aan: All ships of Second Fleet

WGUX DZEXE TEPDR IPPEX KRGQK XIRKQ PWDNZ KWGWK NIXEY PKHKW GSGPG
TETET MXHRK TFPGO KWIQS KPGTA QEZGT DIPPG TCOFT GYKNI GZGGN FPDZM
QERII XAEWG WKTKP EPETG MZKDS EWMUE XEUEY KPEQK UFPEW DEPKH FYFPI
YHTGP EQEXP MZKPE PGNKP KPPEX HRKPE WCPMY YKPBP KPMWK NAWKT GNIQE
ZEPFQ GXXEG TKWEP HYHYE RGVJV

PEARLHARBOR-2 September 9, 1941

van: Chief of Staff, Combined Fleet

aan: All Chiefs of Staff and Commanders

SCXPX CRDZM XFPIP KPAPF ZNPKO HSKRG XHQM W ISMNG SPSDY NEPEP FWKWK
QKNHW INOKE MWKPC TKWEX DXKUB SKMXF WGPBX DXEPK PEYKW APPGU EPKXK
NKTEU FZGPG PXKRE THTKP EPDSG RMWEK NGEPK WEWHX GZEZI YKSIF ZEGTM
OGPEP KREYE PEYGG KXDIP GPGZK PBPKW HNEPK AQKRK WEZCW KZKPE SEFRE
GEPER FZKOG TGXGT GPKMP WKS BX GPCR F PGZGR FREZT FPKXG PGTEX AOGTK
NWN GZ GPKWG SGOKZ ETGXS FXMOG PFWGQ CTKTA UMNKY XGKWG NDWDP ENGRF
PDXKP DVJVJ

PEARLHARBOR-3 October 6, 1941

van: First Air Fleet Staff

aan: Commander Carrier Division 2

Kagoshima Air Group Commander

Commander Carrier Division 1

Commanding Officer Yuuzuki

Combined Fleet Staff

RKPEG REWEZ EXEOE OGYKR EPHEE PYEZD PEPKR BPEUM NETKX ITOIP FZESE
ZCNEP GWCPE PKTER PDYKP GWKRE WFPGR KYBYG KPGPK RGXGS DTKZM RGYKE
RTHKT KTEPG SKWEP HXKWE WKG GZ PEUGZ MPEUG RGOKP GWDYS XDGZG TEXGW
MTEWA PGWEW KEKWW KPFPI QEREP GYKWB OHWXG RDPMN DNENG UCPGP GWPPE
IXBPG SBREP GPEYK PKPKG NXEOH SEPFQ EOFWH RKXGX EYTGT GYKZI ZGWKX
KXEPK TEHZG NGXLP FPGPK WBTFY HAFPE RGPEY KWETB PGRGR GTRPZ ESKXE
PGPGY EYHXK PKZWK KOBSK ZBSKZ EWKXK YEXKV

PEARLHARBOR-4 October 28, 1941

van: Chief of Staff First Air Fleet

aan: Chief General Affairs Section Naval Technical Bureau

General Affairs Section Aeronautics Bureau

Chief First Section Naval Section Imperial Headquarters

Chief Second Section Naval Section Imperial Headquarters

XGTKH WKPFR HWIXE WENBP MTEBK SRGZK ZETFN KPEWG WDUEQ GKPPG YKXMR
FUKOG XKTGR ETHKP GYOGT KXEYE TGUGT GZKUE XEETG TKXGY GXFUM ZCPEP
KYKXZ HKXFP GWMUG WHWGW BSGPE GETOI YKTMZ KSGRF PEYEU IRESX IKPIN
KQIYF NEPGQ MPETE OBFUP KSFYK XDSHP BYBPK PGT OB PKPEP ERKZC REXER
KYPXD EOBRK OKZKP DXEPK WEPDP KSZKO GPEXG PKQEP KTGPE WKPUE XEWKW
KYMPA SEPGP GPAEG TKWHP INMZG XKWGQ EYKGE PGYGU GXEPE PEPIO ERKTX
TUKPE XGPDP KZKZE QCSIZ YGEPB THSBW HYGOE PGYGZ GWVJV

PEARLHARBOR-5 October 30, 1941

van: Chief of Staff First Air Fleet

aan: Kuroshio Maru or Shinkoku Maru

OIPCD PKSEP ETKYK ZGTMP GUMUG TIPER EWGEP THTGP DUKYE REQEN GPESK
 YMYGP HNBAX PKPER KRGPK RKYDZ KSKTK XEZCR KZIIWH XKXQC NGXEO KXERF
 PKSEP ESHPK XKPKP MFEPF WFPGX MWKUE RHZMW BPKNK UMNGP KUSGE OCOGS
 KTERK YKPGT HXEPI PEQKZ CZKET TDZMQ KYFWG SEPGU HZGPE SKPBU HXEYQ
 OEMRK TKWMY ERKOG YFYEX GRDWI QERKT AHKTU KXCTG ODUW FSGWI PKSER
 GRAPK ZKPGP HXKRG OKPKW KPKYD ZEXMP ETKPG SUGY MXEZM TDTER MPIQG
 PEXHT AWGZK PGPRG TKPGX KOGTK XMPGW MXKTH PGTKX ECNRG ZEPIW KPENE
 NKQBZ EWCPI TETAY GKEYF XHZEN HWEPE TBTFN GPENK XGPFY GGWGP KOKRE
 OGWEN GWKRE NETGX ETGRP OOIW EZETG UKWGP MZBYE WGOKP KXGPF WEKNK
 PGZDX GOGUK OKPKO EYGNM PEUHW

PEARLHARBOR-6 November 3, 1941

van: Yokosuka Military Stores Department Chief

aan: Chief of Staff First Air Fleet

WLZNN BWASA ZENLS LNBRB PINBN EQBTB ZDNAW NNMOL ULRLS LRBRL NBNCT
 KWDZL RLWLX LZMNQ CTQAT KZASK UDRBY APDRL RBPLO LXHYL YLXUL LDNDS
 DOAUL YMZIX BRDZB NKYDN LNDI RDDNL WBZBP CYIRD ZAZBW BNEOL NKYBU
 DPDXQ NIXAT BNKZL QDUAO KNLXL NKUCR DNBZL WBUNB NLULS LZAND XARB
 BNLNG ZMNB LYDTD BODBR BTLSA YLPBN HQANB UINBS LODQB ULOHL NDDRI
 OARBS INDRL WDWB DQGND SBXBP DTHBE UDHPG NLYAN DNAYI TDSCR MSENK
 TSLSZ KTILN DPLTA PCRD BOBNL NESDW ARLNK RDQGS DBBZL TANBR LUEUB
 XAZMU DYBPD TDNKN BZLLR SBZCY BYLXB NLZIZ LWLWB NKTBN EYLN RIXDN
 AWGYL NBUDR AXAND ZEQR IQLTL UKNXS DNBOA XBUBR LXANL XDNGZ BUMSD
 ULWHU RBULO BNAYL YBRDZ DTMND NEYCR LSEPL UDSBR ILZIT LYLS YBNDU
 APGUC TDPIZ BTCOB YDXVJ

PEARLHARBOR-7 November 3, 1941

van: Staff of First Air Fleet

aan: Commander of Seaki Air Base

UBYZP DSBTE NKRDN AWAND OLNLU LTARD XZUCP MYLPK XBNBW BNBPB ZDNBR
 BNLRM PZMNQ DODRG ODXLN ATAUL NLXDP DXLUD NLDLU LNBWM RDZIS BSBPL
 SDXLT BRLPB BNAOL RLNDR MXASL PGQHT DTBOD NDTOR IPEOD NBYBT BNBZD
 TDRLO LQLNL SDNNL ZLNBS LUBTA ZAZLS BZLSD ULQBB LQGBP LRBRD TDRLO
 KOKUL ZDOLS DSDYC NDLYD UIPGP LNAZB OKNDN DNIRH RBSDL AOEIO MSDNK
 YDTBW AXASB UHRDR LNDQB SLZDN DTBNC TBTBT LNBYM XEUMN DWLLD QLNLU
 BNDNB PGNDR ITBZD TCZKR DLOXB NDNAS INIPA NLRIN HNERA OLNBN LRAND
 NDZLN DOKPD NBNBN KYDQM RLRUU LRDNB SDNIP ANANL ZLTMO DNBRC RTBND
 TBXBR DUBPA YLPBR BQBZA NDSBP DNDHQ BRBZL SBNSD BNDNB NBRDN DNBTB
 SVJVJ

PEARLHARBOR-8 November 5, 1941

van: Chief Bureau Military Affairs Section

aan: Chief of Staff First Air Fleet

QMNON INIXK NLPIN DNLQI NMWDY ERLUL ULYGS DUBNB NERDR LNDXD SANKN
 CRBNA RBYWW LNLZL NDRGR DZLSK PMQCN GYBTD YLNLZ CZBRC RDTIY IRDRD
 SBRDP LTEQD OKODO ULUUI ZAULW IYARK SDNBU BNEUM QCUBR BSCNL OBSLS
 MZIUB ZLRDN LWDSD WBOAZ LTRDL DPGPD PLOIP DSDOD PLQKT DZISB PBUAR
 MUIPL NLNBS DULRB SMRDS LYBQB OBNBI NDYDU BRGXG ZENCN MNDND NLRMX
 AZDTL WBZIU EWBRB NDSDN LZLSA NBWLN IPLZN ZBRBN DULZB ZBWBO DTDZB
 NGRDY KUANB NCULY HPDWB XANBS BNLOM WLNHW BNDRH RODNB ZKZLP BNMNL
 ZBQLR BOHNB TKTLN BNLNL YLYBP BNBQD NLNBN LYBNL ZAUBB ESLCQ BRMUL
 NBRDR EUKPD NINLN BRESE NBQBU BNLND ODXBN DSBUB UDPDW BRISL PDWBD
 QITBR ENIPL RGYIN LZINB YDNDS LZBOB RLPCP GXLWD ZBTLR BSDPG SBRLO
 BULAM QLLNL QDQIN LQMPL SBNDT BUDPE WLYDU ANDRD RLNCN BRDUC WGYDU
 LYCNG NLYDU HBUDN BNATG NDTLP ENDTB NLTKO CPBUL NKRDY KUDNB NGPAU
 KPIPL UDNIX LSCNB YBDBN BPLPM SMNBN BNDDB ZENLS LQDTL RANDQ DTBQB
 UCNDR DNLZD ZBUBW ITDNI QLINN BSLOC PANHN DUGXB NBNBT BNDND ULTMP
 GNIRE PLTLQ BTLNB YKYLQ GTEUB RLNLS DNLTD NBNLN ANDQB UDSDW CYBRA
 RLZBZ LNLWB XLSGR LWEPB NLRBN LZBUD YDUZZ BQDTD YDPDS IZLOD XLZLT
 LOHNL NLSBP LZGOD XBRDY LWLNB PLNIX BNANA NDRZG RLUBN LNBSB WKNBQ
 IODNK TGOBO DSAUL YLNLO LOHNL NDUHR DPDSB RBNKO CZLSL RBBYL OETEQ
 BZBRL ZLWBP BWLRB ZBRAS DPISD NLWDU LZCRD QBOCN LQDTL ODNDT BOVJV

PEARLHARBOR-9 November 10, 1941

van: Commander in Chief, Sixth Fleet

aan: Sixth Fleet Submarines

ZLYOS LSXOL WDXQN INXCS PBLIR ABPBW ARQLS DNRDN LLNBD ZBDYK ISATC
BNMLR ALSFE UEELS ADRRL NEOND NHPUL SRKNB NBOTM ESDUA

PEARLHARBOR-10 November 19, 1941

van: Commander in Chief Combined Fleet

aan: All Flagships Combined Fleet

QBNNS GQDOL RISLN BTLND ZBSLN BNLNB RKSDY OTLND QMZBQ LZGZK RLNKP
BNLTK NMUMO GOKOZ ISZGN DPBZD YLNLN DXKOL RGQEN LNDUL NDRNI DMSCU
BYAUM WLNCS BNBNI PBNIR INBRL ZCLUK SLNEX BSLNE NANDR DZLND UDRDY
BPGUZ UBPLQ LNDZD SANDU LQHND YGRLY KOBXL UCRYB ZBNIY DOBOI SGTLY
CTDWB ZCUDP DSLTB IYLLW DQBZB SBZLZ KRLNI OMWLT KPLZL ULTHC ZDDYD
NDSAO DXIQB NDSBO BNISA SLNCW KNDAD XLGNB QMOAU LNBZB SENLT KNCRB
ULNCT BNBBN DNDPB UBNIO GXBYL XIUCN DXDZD RLSBW BBDNC XDXGR INMRL
QEWAX DUEZB RBTAN LSKLZ NLNLP BSFNM TBXBP BZBSD XBYLN EZKOL ZDPLR
BWLNL NLZDT BXCYL SBOMO LPBWG NBQSS BRDNB NDNDY CWDNB RKPBO DRLZD
NLPBT TKSLS LTCNA RGSdq KRLSB UIPDY DSOLO NBNDR LBRKS COLNA ODWIN
DPIWD NGZKS BSIQE XCSVJ

PEARLHARBOR-11 November 20, 1941

van: Commander in Chief Eleventh Air Fleet

aan: Eleventh Air Fleet

ZLRPN LQMPD YKNQL NLPDO LXBZX DWTBN BZLSL TLLLY DRBSD RDPDN LZBRL
NZEQB RINBL NZLUI QGUML DUDCZ LNCUI PBTBL RDNCO BNLLY LDNBN ERLOB
SLQKX LNDNA LBUHY BZLNL PTDOB SDQMR NDOBT LRDSX BNDND TERLT DQLYL
NAWSL LRLZE UCPDR

PEARLHARBOR-12 November 20, 1941

van: Staff Submarine Division Two

aan: Commander Ominato Communications Unit

Yokosuka Communications Unit

Staff Sixth Fleet

Staff First Air Fleet

ULQXS BNLSL UBTBQ NDPBR LOLQB RDXUL YRAND RLNDZ LXMLL NLSEW ENBNA
 RDRLR ANBZI TSSIZ LPEXK PLDUN ASLSM NLQLA DWLBN LSMRD UDSBN LDNCR
 ASLOC UBDXL LXBNN NBRDP AOLSA OEZDP DNDDL PKTLX DSLOA QNDPG ULUAY
 DYHNB NDNAN AQDSR FZBUD NDNAQ BRBNB PBSAN DQODB XIPDR AZCND NVJVJ

PEARLHARBOR-13 November 25, 1941

van: Commander in Chief Combined Fleet

aan: All Flagships

ZLRPN DQDRB PBNCQ KZBRN QLOCX DUDNL NBNMN BRZXD WTLTL UIZLQ CZMZM
 PTLLE SCPLN BNDYB WLNLD PBREN MULTD WGNDS GNZBZ LSLNB QCZDN DRLNU
 DNLPN SMUMS KNDXL DUDDR BZLTL QKZIS MPCBT BLRDN LZBYC NENBQ LTLTY
 LDSLX LODNL YDNLN LLPLW DNEND YMOBN DDNAL BNDSL YMOBN CUDQL LPTDY
 CUBSL SLRGN DXDTN INBSG ZLNBH BODSH SYLPI RLNDN DNBSM URLTD NBNS
 IXBNB RDULN SLLRL QDNDO LOLNB ZLNLV

PEARLHARBOR-14 November 27, 1941

van: Tokyo Communications Unit

aan: All Fleets

Striking force

QGSXN AQLTB SEXIT LNDZC NLTBN LQBXH YHNBH ESBTN WLNHR BRCHA SEOLZ
 DZBRL XDZAU DWENC RBQDP LOZBO QLNCX LYCND RLPDY CZCRL NHNLTY GNLNB
 SDWIW IBMSD YBNLS LRBRM NLYDP MNCRM NESDQ DODWD NDYBN BRLNL SLYBN
 HTDZD SLNAR ARDYL NLOBN LUSZA WBYEN LSBRA WDOLW KODOD ZLNER LULRL
 REWGZ YBNDR DNBDT PMNDU BNBNN SBTIN BTBPD NLNLB BOICR BPLOB QLSDP
 KTLQD TBTLT DUBNK ZLWBR BSMOL IWLRA UBNAX DNCTL ZBPLR LTLPB SDRDR
 AQDTB ALULE RGODY CTBND NLNLN LUCRB RBZLX BTBNI NEZBN DOBNA NLNIX
 LUIND NMNDQ DQGNB NDUGP DTBXL LBYHN ATLXD NEUBT ITBYI ODXCU INDRD
 SBSKO HLZNL RBTIT BTANC TBRDN LNLSB NBTLN LSYBL ZBREU AWDND PBSLN
 ATLNC UINMY AOMUL YLZLN DQLYN NLSLN LWDRB NBNBY BRLND RBNDT LNMZB
 ZBUDX LQLNH NBXER AYBNL TBSLS BXLYL RDZLS MUIND TLRIB YIPLN HRAOB
 QLZBY BWBTK RBNIU BYDQD NLODU

PEARLHARBOR-15 November 27, 1941

van: First Secretary Navy Section Imperial Headquarters

aan: Striking Force

Chief of Staff, Combined Fleet

XBZPY LWMUD OLQLO BZAWD OBTIT DTZOD UBUGU KZMSH RDTAO DPAPL REZWC
 NNMRB YESLN LTAPL RDYLY LZHNB LHOBR LND OA ULNDS BPANL ZBZDN LQHNB
 YBUMN DPAND QESKN LSXWL TBT DN LZLUD PAXCU LXDOB YDSQG OBNLU BTDWM
 OLPDT BTCTD IIQLI SENBX DZLYG PIPLU LPHXI QDRGL NLYDT BRDND ZLSEP
 AYENI QBKGN BBYDX LNDXB YHU DT DRAUB NDZDN LPDZD NLUAO LYDOI NDTLS
 HTILC SCNDT LODZL NBSKY AYLRE NHDNX BOCYB PCXDN BNENA NHYAS BNDXB
 NLYLP DNBQL OAXAZ LXBPH SYXCN MOBRM RLYLR KYDOG YBZLY DRIYB QLNLN
 DOIRK ZDRBO DZDYL OBCZL NKWLZ CZBQB XBOBW LOLT B PVJVJ

PEARLHARBOR-16 December 1, 1941

van: Shiriya

aan: Commander Destroyer Division 7

TDTIK SATBQ HNBRD QENBE ONAOD NMPDN LNEUL PLNSL PDTBN DUDSD YMNDU
 MZRBS BNLT L NDYDU ADBSA QINAZ IRAZB OKLQO MLSAQ DSFZC NMND O EBNTB
 PHSKS INKWB TBXTO DLPBN LNLNE RENLS DILNO LRMWL NLBNB BQDTX LNL SB
 ZDNLZ KNBPN DBNAT BZLZB SBNLN LIUSA NLNCQ BRDTD UBBQT ATLRB NDOMZ
 LTLSB LRBOL OBNMO BZDPH DGNBN MTKXD QIRBW NNYNB YLYLZ KTDSK NCWPC
 KZANM SBRLX AXMYL

PEARLHARBOR-17 December 2, 1941; Top Secret

van: Commander in Chief Combined Fleet

aan: Combined Fleet

ZLYDD QAODR BMMOT BNBUD NADNT BWBSL NAE OB NOKZB UDNIE NBNDR ATKYU
 LIZAQ LRHLZ SMWBP LUZLY DDQAO DRBEO BNOKZ BUDNL CYAND RAYLS DUBOD
 NTBWB SLNAP RKBND NDTAN BLTRE NIQDO ANTLL PBPDR ASMMO TBNBU DNAZB
 DNMNL XAXBN TDSAR DSHIE NBNDR ATUNX PDNBP AXDBZ ANBRB LDSND OFNDN

PEARLHARBOR-18 December 2, 1941; Top Secret - Retransmission

van: Commander in Chief Combined Fleet

aan: Combined Fleet

ZLYDD QAODR BMMOT BNBUD NADNT BWBSL NAE OB NOKZB UDNIE NBNDR ATKYU
 LIZAQ LRHBL TRENI QDOAP RKBND NDTAN LDSND OFNDN YLSDU BONTL LPBPD
 RASLZ SMWBP LUBNT DSARD SHDBZ ANBRB LCYAN DRAUN XPDNB PAXZB DNMNL
 XAXVJ

9.5 Noord Afrika oefening *****

Inleiding

Deze oefening is ontleend aan een Engelse cursus cryptoanalyse uit 1942. De gehele tekst van deze cursus is te vinden in *A Course in Cryptanalysis*, een reprint door Aegean Park Press van *S.I.Course, Revised and Enlarged, June, 1942*. De korte begeleidende Engelse tekst is hieronder overgenomen. Het is een (oververcijferde) code en het hoofddoel is het uitplussen van plm. 70–80% van de oververcijfering. Verder is erg weinig materiaal om het codeboek te reconstrueren. Veel meer dan de groepen voor de letters van het alfabet, enkele lettergroepen en een paar woorden zit er niet in. Al met al is het best een lastige opgave.

The background to this exercise is the early part of the British offensive in Libya in January, 1941, culminating in the fall of Bardia. The messages are supposed to be Italian, taken by our Interception Service. The contents are imaginary, but more or less realistic, and the text is English.

You may expect the Italian commanders concerned to use signatures and addresses as a regular practice. The following extracts from the Italian Order of Battle published by the Intelligence Branch of the General Staff may be of assistance:

ANTONELLI	General	Intendant-General(Supplies)	at BENGHAZI
ARGENTINO	General	Commanding Defences	at DERNÀ
BERGINZOLI	General	Commanding Defences	at BARDIA
GALLINA	General	Intendant-General(Supplies)	
		C-in-C, Eastern Libya	
		at advanced GHQ	at TOBRUK
LEO	Lt-Col	OC, Saharan Battalion	at HON
RUFFO	Col	Second in Command	at DERNÀ

The Wireless Intelligence Service has provided the following identifications of the Italian W/T stations concerned:

W/T Station	Identification
X	Advance HQ, E. Libya, near TOBRUK
Y	BENGHAZI area (Probable)
Q	DERNÀ (Probable)
S	HQ, BARDIA
N	TOBRUK (Probable)
O	Believed to be a form of CQ (all stations) call, since traffic is always to O, and never originates there
P	HON

Write a description of the different processes used and of the indicating systems, and build up the original book or books as far as possible. Describe also the reasoning you used in arriving at a solution.

Berichten

NOORDAFRIKA-1 Date: 1/1 Intercept: 0900

van: Station X

aan: Station Y

78901 60730 74769 85760 97799 11228 73928 65464 05744 50524 78007
09597 84359 22385 12393 78565 32842 75017 62630 71764 40992 33739
75938 69713 19298 08276 89338

NOORDAFRIKA-2 Date: 1/1 Intercept: 0930

van: Station Y

aan: Station X

34567 60730 74769 84260 03391 18187 52608 65464 17243 64171 07778
09597 48828 00755 53504 79786 97224 06828 90818 47758 84147 31012
75938 79319 69898 42339

NOORDAFRIKA-3 Date: 1/1 Intercept: 1100

van: Station Y

aan: Station X

23456 51747 33040 45035 92588 93926 02329 56912 57146 73077 56769
67046 94811 51690 43998 23359 04198 80160 09597 19716 38488 39968
26233 15224 21026 14932 04830 92822 18800

NOORDAFRIKA-4 Date: 1/1 Intercept: 1200

van: Station N

aan: Station O

00000 21388 75980 09987 18562 54198 11084 46613 11533 42010 73917
31834 77584 25231 53285 88416 00894 34207 09962 55107 00510 94490
43118 28374 10746 36417 62180 44245 55171 39375 98051 90702 26242
84663 85047 90709 26240 44842 55135 42507 93162 61012 08101 22712
33316 71296 65938 22762 33338 47937 75972 22900 56030 84258 50890
09751 47309 53375 30951 59811 50224 96899 07317 72856 36254 50495
35184 40023 48499 99003 74415 11805

NOORDAFRIKA-5 Date: 1/1 Intercept: 1200

van: Station X

aan: Station CQ

67890 85486 47842 72346 65464 70505 29830 87014 09597 71500 04932
97336 96649 90441 39903 49020 71683 52245 95650 75938 06160 08357
23453 48538 81390 02576 99476 53296 65187 01785 36730 27130 81966
40334 41596 62200 13486 20413 54299 46827 27509 08884 34096 68086
35763 51971 17318 14421 64417 12223 47187 15415 47831 74294 63677
07102 37759 33428 58806 74165 00369 77177 75296 56788 59874 21793
72055 51552 40147 10058 24017 93636 26300 34722 08346 28735 36404
04985 64758 39284 96522

NOORDAFRIKA-6 Date: 1/1 Intercept: 1700

van: Station X

aan: Station Y

12345 79790 06707 10217 63743 40357 60398 11887 47678 55827 51709
95294 75938 26264 42279 05420 42644 76095 54808 08066 43865 38400
68997 36730 41301 30513 40235 79296 23341 95497 41487 60109 56671
75931

NOORDAFRIKA-7 Date: 2/1 Intercept: 1200

van: Station N

aan: Station O

00000 21388 75980 44010 88488 04010 80086 89054 39823 79278 26590
39940 43131 83413 41401 89989 55587 59811 50244 85833 54220 08686
18073 31834 77584 25231 53285 58327 02484 24687 66120 33992 00312
24103 53463 44217 99232 61012 08101 22710 33314 71296 65938 22713
33316 85330 02361 39375 98051 90742 26217 84663 85047 90762 26212
36011 92403 14384 54683 06696 74423 95398 39231 23096 32993 50602
86357 98842 55747 00243 55983 08718 92949 94490 43118 00677 45747
79769 18059 08737 71120 42084 15901 42462 93639 39286 19584 68115
02849 24021 63529 19266 83498 30453 91160 86733 66301 44710 88393

NOORDAFRIKA-8 Date: 2/1 Intercept: 1200

van: Station X

aan: Station CQ

34567 83185 93757 32758 87550 31934 14969 29692 23363 60274 81885
09597 56195 88927 00084 83234 18783 08863 78992 00915 01348 09118
75938 24194 08438 05789 88902 96446 51788 31508 44590 76924 61728
36730 74908 69899 40415 22223 57276 57896 20323 28133 46827 27509
08884 34096 88868 66886 95886 45027 87152 04412 12133 11021 15415
47831 74200 63686 61738 80503 26026 53883 55341 03734 57191 08894
56788 81671 00454 16951 68942 54137 54707 47383 97777 17927 01109
08346 52660 69815 94749 42416 52566 19857 13846 32538 49485 89015
72296 28563 89954 80941 85636 26488 22813 44911 25161 35910 62200
78968 40436 59777 97021 00194 08563 02651 88039 15573 76585 16901

NOORDAFRIKA-9 Date: 2/1 Intercept: 1900

van: Station Y

aan: Station X

45678 27678 86657 85127 09743 50429 52304 42160 62278 10915 35347
89450 72296 49146 98213 25433 01091 92472 67275 70753 76254 77776
68076

NOORDAFRIKA-10 Date: 3/1 Intercept: 1100

van: Station Q

aan: Station P

00000 47039 47124 87057 81440 59500 37134 40452 95726 22773 33306
22772 33306 43769 22367 30912 23938 92842 45442 63306 18447 00203
55463 89546 03256 62701 93387 47957 56542 52461 35134 63029 00598
93272 62725 11364

NOORDAFRIKA-11 Date: 3/1 Intercept: 1200

van: Station N

aan: Station O

00000 21388 75980 09987 18562 91842 97538 17722 64318 33230 00454
39039 68539 09612 57916 79479 95167 20190 55088 76089 28079 47545
19419 63281 63442 81194 25979 32175 10780 39412 65663 80494 85667
40023 48499 99003 74415 11863

NOORDAFRIKA-12 Date: 3/1 Intercept: 1200

van: Station X

aan: Station CQ

23456 88476 26633 34123 40178 62293 83786 64990 78893 89717 38014
02400 56912 57155 47135 70400 87569 84180 00854 12944 18406 34459
79225 09597 73316 05660 16641 31186 37132 26961 65220 60869 71596
65982 75938 45328 08438 11367 53532 99303 10830 02314 75658

NOORDAFRIKA-13 Date: 3/1 Intercept: 1300

van: Station X

aan: Station Y

56789 77418 56912 55401 23130 05042 22899 08618 97104 09620 49527
95207 50656 08547 09597 81528 74554 53504 92227 65071 32860 99163
90656 15734

NOORDAFRIKA-14 Date: 3/1 Intercept: 1600

van: Station X

aan: Station Q

67890 82825 75938 03447 14724 18774 59512 55925 78320 76911 41828
89803 65060 70915 36730 31382 03546 40424 43631 73327 81818 20387
68171 69152 31762 08884 86724 06233 88907 72116 45883 19701 50827
27298 16468 59362 47831 45300 12829 92523 02090 82206 45042 26325
04697 05236 92941 56788 13846 79249 58757 16784 41738 31940 17632
78394 94186 49689 08346 52660 18029 98855 08999 14665 99640 46021
10956 60770 17815 72296 05306 95232 07828 53760 91315 49149 05595
45609 73039 30727 78968 90194 07645 66919 21177 60802 32317 20881

NOORDAFRIKA-15 Date: 3/1 Intercept: 1730

van: Station Q

aan: Station X

12345 93205 29567 49097 61498 79034 57357 57180 20323 23570 81265
59019 08884 34951 35339 11080 39132 97787 91140 04594 39477 99025
85071 47831 22198 55249 15117 43616 26038 31023 82412 00853 89695
17876 56788 32008 20530 35625 01877 90742 49854 49894 38560 43563
52956 28816 08346 96517

NOORDAFRIKA-16 Date: 4/1 Intercept: 0630

van: Station Q

aan: Station X

23456 71390 30934 45914 31563 01839 26488 36266 48201 02260 76842
33636 78968 74472 23223 19621 87995 19234 20686 45136 74412 24455
86493 56912 74309 91669 69083 79291 73568 28854 75700 22645 05583
90584 64880

NOORDAFRIKA-17 Date: 4/1 Intercept: 1200

van: Station X

aan: Station CQ

45678 06788 67332 09839 20013 09597 92628 58839 43662 22897 17048
60039 01655 84734 74917 69126 75938 25178 96522 43051 15871 31467
17429 93788 14997 65187 19066 36730 19431 89180 02514 26776 14358
22459 35357 34441 09782 34989 08884 52103 39614 39270 08245 94260
10431 48702 12214 83552 52147 47831 67610 63497 14594 75579 89892
12916 97446 04794 72325 25204 56788 07385 83892 75765 45195 72085
49728 24022 50062 27248 95594 08346 04073 68877 30482 96447 52566
86992 41511 99871 29548 17648 72296 57638 93647 68574 08687 17014
39374 56639 22602 40914 70213 78968 32423 90932 75623

NOORDAFRIKA-18 Date: 4/1 Intercept: 1200

van: Station N

aan: Station O

00000 21388 75980 74006 15426 64834 89020 31384 99398 08718 92949
94457 43192 91850 90213 58594 30248 28807 49010 23147 97949 25972
53084 29734 16187 26103 43776 54198 11084 03512 93107 98350 30353
31834 77584 98528 95389 33258 41785 91152 67922 44018 88484 11148
10253 37201 66039 83763 89077 67272 69437 99373 33908 44010 88488
78207 06423 82065 69523 37234 66155 10512 22133 79278 26590 39940
43131 30481 05164 33922 22954 84315 44550 23308 67045 18168 55008
76528 10566 49364 97937 40023 48499 99003 77415 11860

NOORDAFRIKA-19 Date: 4/1 Intercept: 1630

van: Station Q

aan: Station X

56789 06441 89418 91468 84355 75498 82206 07408 08577 57290 10435
52639 56788 78449 53531 15104 39065 54446 18307 59348 74876 39324
00716 08346 62087 24802 13109 01136 73214

NOORDAFRIKA-20 Date: 4/1 Intercept: 1700

van: Station S

aan: Station X

89012 13667 74422 09942 61114 58774 78168 02576 07551 43865 76924
61728 36730 16028 66495 24853 84149 09689 22683 20323 21245 29739
47022 08884 82071 31613 79059 43139 50007 07484 07101 27078 20218
92134 47831 18576 49284 58574 72333 44305 02095 97571 99387 10260
25204 56788 63375 98430 19149 02646 56690 31931 20409 72019 39243
82716 08346 49859 70204 83821 49780 44138 57924 22564 47562 62651
91786 72296 10144 63305 60912 01910 26488 23020 67596 72691 69334
59050 03458 78968 34933

NOORDAFRIKA-21 Date: 4/1 Intercept: 1830

van: Station X

aan: Station S

78901 38482 97787 01247 54761 40195 91932 49674 73800 27054 16174
02063 08346 30359 25401 57776 44284 33053 42160 55690 42953 60245
02579 72296 05225 92627 10409 01091 92472 73877 77612 60934 56456
68146

NOORDAFRIKA-22 Date: 5/1 Intercept: 0700

van: Station S

aan: Station X

67890 60730 74769 08760 03391 18187 52608 65464 71543 87203 79225
09597 82140 45666 02756 84284 31450 97241 90818 59426 32338 17817
75938 17283 97533 42961 04438 25035 52867 10494 51954 17419 10857
36730 18954 03645 31439 84149 09689 49017 20404 09860 31893 89332
08884 02142 95240 51771 46489 23198 70621 79538 63421 27801 75656
47831 98887 63596 35519 25954 40257 53883 39073 75669 05236 72911
56788 69119 99501 43804 90106 67638 65837 18061 52002 28044 73169

NOORDAFRIKA-23 Date: 5/1 Intercept: 0730

van: Station X

aan: Station S

12345 86714 66802 86317 82621 90981 52159 75938 48550 08438 45193
22732 56854 02495 19769 78117 65961 41821 36730 56164 95398 49245
48749 34158 61477 07169 90806 19054 58938 08884 06809 80402 50763
38802 13359 87186 35420 86088 54569 81059 47831 30457 39661 89113
96633 02599 82044 97857

NOORDAFRIKA-24 Date: 5/1 Intercept: 0830

van: Station S

aan: Station X

34567 09659 08346 24805 28735 36404 04985 39284 52566 11297 78420
30525 62677 85249 72296 74621 06765 88821 89609 02095 21802 56639
03217 78968 59159 78968 48188 28769 00719 00013 42813 09082 17410
35872 72943 12725 56912 22897 70210 08694 52962 96934 67027 70558
16312 49097 12685 09597 19627 27004 22057 07152 11901 11887 66802
82621 90981 52159 75938 64071 48550 42274

NOORDAFRIKA-25 Date: 5/1 Intercept: 1200

van: Station X

aan: Station CQ

23456 83185 93757 33758 87550 50241 67713 14676 96743 83197 33083
09597 82140 45666 02756 84284 31450 97241 47116 34577 89082 04543
75938 97686 56422 92853 88908 78320 64675 22322 65604 56101 63601
36730 79543 73187 19968 44143 30747 84730 00594 56608 19636 41108
08884 34906 80402 04960 51971 12755 59869 26246 80022 97715 95764
47831 45435 40196 26419 80503 74878 26631 88157 90221 05317 02642
56788 28462 48531 93195 08232 56546 14266 49894 39181 55307 79983
08346 52561 08847 27561 07965 52485 42160 39425 58450 78896 02533
12276 72296 49371

NOORDAFRIKA-26 Date: 5/1 Intercept: 1200

van: Station N

aan: Station O

00000 21388 75980 06957 12450 22288 60115 55305 00685 16057 74530
22248 60115 20361 17114 18904 54478 63945 63933 73249 91816 39490
43441 29972 54088 25552 16240 77802 16435 23308 67045 47993 11631
91662 51608 12870 75061 44081 55657 34207 09962 36417 62180 33141
99371 20610 51275 08772 40373 83995 24072 28041 41271 83738 37015
02192 58153 02790 53311 20275 44907 10266 85569 42166 93556 45574
11879 92841 69492 22751 35924 35543 52956 04503 59434 30453 91160
86733 66301 44726 88317

NOORDAFRIKA-27 Date: 5/1 Intercept: 1210

van: Station S

aan: Station X

For General GALLINA. I have given orders to cease resistance.
General BERGINZOLI. 18.

NOORDAFRIKA-28 Date: 5/1 Intercept: 1230

van: Station X

aan: Station CQ

56789 22805 31046 51021 30738 39026 24642 78968 66188 42518 66151
45355 32399 35062 01897 10586 40462 02400 56912 57146 95948 73602
53544 13945 73843 65202 18406 72170 97750 09597 70108 18247 53423
18805 92398 06089 90818 47758 85865 33971 75938 83991 08258 89110
57869 37845 12396

NOORDAFRIKA-29 Date: 5/1 Intercept: 1230

van: Station Q

aan: Station X

12345 52487 63198 61691 78601 86447 18244 72350 47851 09597 15600
43783 78345 47196 49230 87871 00154 85903 90641 92132 51777

A

Tabellen

Vigenère tabel

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

Beaufort tabel

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

Beaufort tabel Hagelin M-209

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0,26:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
1,27:	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
2:	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
3:	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
4:	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
5:	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
6:	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
7:	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
8:	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
9:	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
10:	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
11:	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
12:	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
13:	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
14:	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
15:	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
16:	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
17:	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
18:	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
19:	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
20:	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
21:	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
22:	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
23:	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
24:	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
25:	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z

Porta tabel

	A	B	C	D	E	F	G	H	I	J	K	L	M
AB:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	A	B	C	D	E	F	G	H	I	J	K	L	M
CD:	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
	A	B	C	D	E	F	G	H	I	J	K	L	M
EF:	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
	A	B	C	D	E	F	G	H	I	J	K	L	M
GH:	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
	A	B	C	D	E	F	G	H	I	J	K	L	M
IJ:	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
	A	B	C	D	E	F	G	H	I	J	K	L	M
KL:	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
	A	B	C	D	E	F	G	H	I	J	K	L	M
MN:	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
	A	B	C	D	E	F	G	H	I	J	K	L	M
OP:	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
	A	B	C	D	E	F	G	H	I	J	K	L	M
QR:	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
	A	B	C	D	E	F	G	H	I	J	K	L	M
ST:	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
	A	B	C	D	E	F	G	H	I	J	K	L	M
UV:	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
	A	B	C	D	E	F	G	H	I	J	K	L	M
WX:	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
	A	B	C	D	E	F	G	H	I	J	K	L	M
YZ:	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

Frequentietabel Engels

	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	%	
A-	4	20	28	52	2	11	28	4	32	4	6	62	23	167	2	14		83	76	127	7	25	8	1	9	1	8.0	
B-	13				55				8	2		22			11			15	4	2	13				15		1.6	
C-	32		7	1	69			33	17		10	9	1		50	3		10		28	11				3		2.8	
D-	40	16	9	6	65	18	3	9	56		1	4	15	6	16	4		21	18	53	19	5	15		3		4.0	
E-	84	20	55	125	51	40	19	16	50	1	4	55	54	146	35	37	6	191	149	65	9	26	31	12	5		12.9	
F-	19	3	5	1	19	21	1	3	30	2		11	1		51			26	8	47	6	3	3		2		2.6	
G-	20	4	3	2	35	1	3	15	18			5	1	4	21	1	1	20	9	21	9		5		1		2.0	
H-	101	1	3		270	5	1	6	57				3	2	44	1		3	10	18	6		5		3		5.4	
I-	40	7	51	23	25	9	11	3			2	38	25	202	56	12	1	46	79	117		22		4		3		7.8
J-	3				5				1						4						3						0.2	
K-	1				11				13					2	2				6	2	1		2		1		0.4	
L-	44	2	5	12	62	7	5	2	42	1	1	53	2	2	25	1	1	2	16	23	9		1		33		3.5	
M-	52	14	1		64				3	37			7	1	17	18	1	2	12	3	8		1		2		2.4	
N-	42	10	47	122	63	19	106	12	30	1	6	6	9	7	54	7	1	7	44	124	6	1	15		12		7.5	
O-	7	12	14	17	5	95	3	5	14		19	41		134	13	23		91	23	42	55	16	28		4	1	6.6	
P-	19	1			37			4	8			15	1		27	9		33	14	7	6						1.8	
Q-																					17						0.2	
R-	83	8	16	23	169	4	8	8	77	1	10	5	26	16	60	4		24	37	55	6	11	4		28		6.8	
S-	65	9	17	9	73	13	1	47	75	3		7	11	12	56	17	6	9	48	116	35	1	28		4		6.6	
T-	57	22	7	1	76	5	2	330	126	1		14	10	6	79	7		49	50	56	21	2	27		24		9.7	
U-	11	5	9	6	9	1	6			1	19	5	31	1	15			47	39	31		3					2.5	
V-	7				72				28						5										3		1.2	
W-	36	1	1		38			33	36			4	1	8	15				4	2			1				1.8	
X-	1		2			1			3						1	5				3			1				0.2	
Y-	14	5	4	2	7	12	2	6	10			3	7	5	17	3		4	16	30			5				1.5	
Z-	1				4																						0.1	
	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z		

hoog	hoog-hoog		hoog-laag		trigram	woordscheiding
TH = 730	ER = 191	RE = 169	HE = 270	EH = 16	THE = 233	beginletters: TOAWBCDSFMRHIY
HE = 270	ES = 149	SE = 73	EA = 84	AE = 2	AND = 90	
IN = 202	EN = 146	NE = 63	TH = 330	HT = 18	THA = 50	slotletters: ETDNSRY
ER = 191	TE = 76	ET = 65	IN = 202	NI = 30	ENT = 59	
RE = 169	AN = 167	NA = 42	NC = 106	GN = 4	ION = 49	
AN = 167	ON = 134	NO = 54	HA = 106	AH = 4	TIO = 43	
ES = 149	AT = 127	TA = 57			FOR = 42	
EN = 146	TI = 126	IT = 117			NDE = 40	
ON = 134	ST = 116	TS = 50			NTH = 30	
AT = 127					HAS = 29	

Frequentietabel Nederlands

	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	%
A-	110	2	37	33	1	22	13		3		10	72	10	257	1	19		68	7	62	2	6	3			3	7.4
B-	14	8			64				3			6			10			19	1	2					18		1.4
C-	1		1	5	1			91	4			2	10		15	1				16		2					1.5
D-	49	2	3	8	334		5	9	83		3	3	7	2	35			18	12	17	5	10	4			4	6.1
E-	37	47	38	79	165	15	66	31	62		30	137	42	470	21	29		272	79	126	19	102	24	3	30	19.2	
F-	3	4		11	6	3	6		4		5	1		1	3			5	4	9	1	3			1	0.8	
G-	17	1	1	8	213		7	7	21	1	2	4	5	3	8			17	17	16	4	16	5		1	5	3.8
H-	22			4	105		1		12		2				18			2	2	56	6	2			9	2.4	
I-	6		14	23	122	3	60				8	24	9	166	3	2		4	49	45	2	11	1				5.5
J-													1		5					1							0.1
K-	21	4		2	56		4	2	16		9	3	5	2	16	3		12	8	16	4	3	7		1	1.9	
L-	52	3		28	81	1	15	3	26	5	12	43	2	3	22	1			20	9	10	11	5	49	3	4.0	
M-	46	1		13	51	1	1		11				4		29	3			5	3	5	3			2	1	1.8
N-	44	22	21	212	90	19	123	35	79		26	12	18	35	46	7		15	52	88	10	73	30		47	11.1	
O-	1	1	3	11	65	11	12		3		8	25	32	89	81	49		97	10	26	11	19			1	2	5.6
P-	15	3		8	53		4	6	8		2	18	2		13	7		7	2	5	3	5	3			1	1.6
Q-																											0.0
R-	29	33	2	87	79	1	22	16	68		19	7	13	10	52	11		8	34	35	12	20	12		17	12	5.9
S-	11	8	23	18	35		13	10	17		4	15	3	11	19	17			10	122	2	14	8		5	3.6	
T-	69	9	1	36	191	1	12	24	70		6	13	12	3	43	12		24	46	24	8	31	25	1	6	12	6.8
U-	1		5	4			4	1	29		5	11	2	21		1		17	3	2	15	3	10				1.4
V-	108			1	106				16			6	1		65			3			10		1		24		3.4
W-	46	1		1	50		1		6		1				31			1	1				1		8	1.5	
X-					1											2					1						0.1
Y-	18	2		17	4	3	10	6		1	42	2	1	34	6	1			3			9	1		6		1.7
Z-	12				51				11			2		1	15						1	5	1	5	31		1.3
	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	

hoog	hoog-hoog		hoog-laag		dubbel	trigram	
EN = 470	EN = 443	NE = 90	ND = 212	DN = 2	EE = 165	VAN = 104	AAN = 51
DE = 334	DE = 334	ED = 79	NG = 123	GN = 3	AA = 110	GEN = 99	RDE = 49
ER = 272	ER = 272	RE = 79	VA = 108	AV = 6	OO = 81	DEN = 84	AAR = 48
AN = 257	GE = 213	EG = 66	NT = 88	TN = 3	LL = 43	EEN = 74	OOR = 47
GE = 213	TE = 191	ET = 126				ENT = 72	STE = 46
ND = 212	EL = 137	LE = 81				NGE = 70	NVA = 45
TE = 191	IE = 122	EI = 62				VER = 70	EST = 44
IN = 166	VE = 106	EV = 102				AND = 67	LLE = 43
EE = 165	AN = 257	NA = 44				END = 63	ENG = 40
EL = 137	IN = 166	NI = 79				TEN = 61	ENE = 40
EI = 126	ST = 122	TS = 46				ENV = 59	

Frequentietabel Duits

	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	%
A-	6	29	35	12	60	14	20	11	5		1	62	12	82		3		41	52	41	63	1	1			1	5.5
B-	6				104	2	2		8		1	6		1	4			3	2	7	8		1			1	1.6
C-								280			14																2.9
D-	65	5		10	233	2	2	2	86	1	3	4	5	6	11	1		9	13	3	16	3	7		6		4.9
E-	20	62	20	67	35	38	73	75	242	3	19	62	45	443	4	9	1	375	168	47	52	20	26			12	19.2
F-	26	1		7	44	17	6	2	8			8		3	7			11	5	27	21		2			1	2.0
G-	21			12	196	2	5	2	15			13	18	2	9	2		13	16	11	13	2	3			5	3.6
H-	71	3		16	124	2	6	1	38	1	3	33	13	23	13	1		61	17	61	14					1	5.0
I-	5	4	95	11	188	11	53	32		1	2	32	10	197	5			26	72	63		3	8			3	8.2
J-	4				12																						0.2
K-	18			3	28	1	4	1	3			11			15			25	5	8	7	2	1			1	1.3
L-	46	4		17	73	4	13	4	67		6	36	3		8				26	25	11	3				2	3.5
M-	31	2		2	39		4	2	22		1	1	13	1	3	6		2	10	7	14	4	4			1	1.7
N-	57	25	1	208	143	17	102	27	75	4	31	7	18	34	14	3		8	84	49	43	14	22			34	10.2
O-			13	8	30	6	3	6	3		1	21	9	35	2	5		32	14	19		3	1			3	2.1
P-					4	18		1	4			3				1	3		12		2	2					0.5
Q-																					1						0.0
R-	63	5	16	54	124	12	25	24	61	2	26	17	10	32	19	6		21	55	43	48	5	20			13	7.0
S-	24	4	105	19	113	12	20	10	76	2	10	6	4	7	45	13			82	118	13	9	7			8	7.1
T-	51	5		40	178	11	6	16	45	2	2	11	11	7	9			32	48	28	33	10	19			22	5.9
U-	2	7	9	4	81	27	16	6	2			8	14	139		4		30	38	22	1	5	4			3	4.2
V-					38				9						37												0.8
W-	31				50				40						13						4						1.4
X-																											0.0
Y-																											0.0
Z-	3			1	21				12			2		1	2						5	58		12			1.2
	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	

hoog	hoog-hoog		hoog-laag		trigram
EN = 443	EN = 443	NE = 143	CH = 280	HC = 0	EIN = 120
ER = 375	ER = 375	RE = 124	ND = 208	DN = 6	SCH = 105
CH = 280	EI = 242	IE = 63	SC = 105	CS = 0	DER = 97
EI = 242	DE = 233	ED = 67	NG = 102	GN = 9	ICH = 92
DE = 233	IN = 197	NI = 75			NDE = 89
ND = 208	GE = 196	EG = 73			CHE = 83
IN = 197	TE = 178	ET = 47			DIE = 76
GE = 196	ES = 168	SE = 113			INE = 70
IE = 188	UN = 139	NU = 43			DEN = 67
TE = 178	HE = 124	EH = 75			GEN = 65
	ST = 118	TS = 48			
	AN = 82	NA = 57			
	SI = 76	IS = 72			

Frequentietabel Frans

	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	%
A-	3	23	35	14	3	13	30	2	117	2		54	17	130		26	1	86	52	56	64	35				5	7.7
B-	12				13				10			20			7			12	3	1	1	1					0.8
C-	18		8	1	98			40	28			12			87			11	5	8	14				2	3.3	
D-	35				215				2	33			1		21		1	12	4		35	1					3.6
E-	53	14	100	96	66	33	14	1	16	12		141	113	242	15	82	31	163	305	143	89	24		17		6	17.8
F-	23			1	11	10			17			8			14			19	1		2						1.1
G-	11				48		1		12			7		7	2			13	1	2	5				1		1.1
H-	12				33				10						7						2						0.6
I-	14	3	22	17	94	8	8		2			65	35	90	49	14	15	51	103	112		13		8			7.2
J-	2				9										4						4						0.2
K-																											0.0
L-	101	1	1	5	246	2	3	4	47			66	1	4	38	3	2	4	10	6	40	2			3		5.9
M-	55	15			104				25			20			22	29				2							2.7
N-	30	2	60	80	124	11	29	3	22			7	7	24	37	21	9	3	79	197	5	10			1		7.6
O-		4	7	2	3	5	2		52	2		29	38	164		17	3	47	22	11	118	1			7		5.3
P-	78			2	49			4	6			42			51	16			52	4	3	17					3.2
Q-																					134						1.3
R-	92	1	27	20	209		7	1	69			35	13	15	55	12	8	17	39	41	13	5			1	1	6.8
S-	75	9	36	57	155	15	10	1	64	2		44	11	13	60	39	40	9	73	61	39	9			1		8.2
T-	85	4	16	45	163	5	2	4	98	1		30	3	10	39	28	18	86	42	29	18	4					7.3
U-	21	3	16	15	85	2	2		68			24	12	62	1	20	3	88	76	56	3	19		29			6.0
V-	33				38				24						23			7			2						1.3
W-																											0.0
X-	6	1	3	5	3	2	1	2	2			4	1		2	16	3		1	1	1						0.5
Y-	8		1		5		1					1						1	3	1							0.2
Z-	1				2				1												3						0.1
	-A	-B	-C	-D	-E	-F	-G	-H	-I	-J	-K	-L	-M	-N	-O	-P	-Q	-R	-S	-T	-U	-V	-W	-X	-Y	-Z	

hoog	hoog-hoog		hoog-laag		trigram	woordscheiding
ES = 305	ES = 305	SE = 155	NT = 197	TN = 10	ENT = 118	beginletters:
LE = 246	LE = 246	EL = 141	ON = 164	NO = 37	LES = 77	PASMCEDTVFR
EN = 242	EN = 242	NE = 124	QU = 134	UQ = 3	QUE = 72	
DE = 215	DE = 215	ED = 96	AN = 130	NA = 30	EDE = 58	slotletters:
RE = 209	RE = 209	ER = 163	IE = 94	EI = 16	MEN = 54	ESTRNDIAIXZ
NT = 197	TE = 163	ET = 143			LLE = 53	
ON = 164	EM = 113	ME = 104			DES = 50	
ER = 163	IT = 112	TI = 98			TRE = 49	
TE = 163	IS = 103	SI = 64			ELE = 47	
SE = 155	LA = 101	AL = 54			EME = 47	
	EC = 100	CE = 98				
	RA = 92	AR = 86				
	TR = 86	RT = 41				
	TA = 85	AT = 56				
	PA = 87	AP = 26				
	US = 76	SU = 39				