

Codetheorie: Ontcijfer opdracht

Robin Verachtert - s0121405

26 march 2015

Contents

1	Vigenere	3
1.1	Opdracht	3
1.2	Ongedaan maken van de kolomtranspositie	3
1.3	Vigenere oplossen	4
2	Playfair	5
2.1	De opdracht	5
2.2	Poging 1: frequentie analyse	5
2.3	Poging 2: slimme frequentie analyse	6
2.4	Poging 3: Hill Climb Algoritme	6
2.5	Poging 4: Churn Algoritme	6
2.6	De encrypted text	8
3	ADFGVX	9
3.1	De opdracht	9
3.2	Morse decoderen	10
3.3	De kolomtranspositie	10
3.4	Vinden van de taal.	10
3.5	Vinden van de bron tekst	11
4	Enigma	12
4.1	Opdracht	12
4.2	Een beetje extra onderzoek	12
4.3	Maken van de Enigma machine	13
4.4	Crib graph en begin positie van de rotors	13
4.5	Bepalen van het plugboard en ontcijferen van de tekst	14
	Appendices	16

A	Oplossingen	16
A.1	Vigenère	16
A.2	ADFGVX	17
A.3	Playfair	18
A.4	Enigma	20
A.5	Diffie Hellman	21

1 Vigenere

1.1 Opdracht

De eerste ciphertekst was versleuteld met een Vigenère cipher gevolgd door een enkele kolomtranspositie. Bij het ontcijferen moesten we dus eerst de kolomtranspositie ongedaan maken om een ciphertekst te bekomen die enkel met Vigenère versleuteld was.

1.2 Ongedaan maken van de kolomtranspositie

We zochten een manier om snel te checken of een ciphertekst met Vigenère versleuteld was, zodat we de kolomtranspositie konden bruteforcen in een haalbare tijd. Hiervoor vonden we de "index of coincidence" (IC). Deze wordt als volgt berekend: $IC = \frac{\sum_{i=1}^c n_i(n_i-1)}{N(N-1)/c}$ met n_i de frequenties van de c verschillende letters in een tekst lengte N . In essentie is dit een frequentietabel samengevat in 1 waarde. Hoe groter de IC, hoe groter de kans dat twee willekeurig gekozen letters in een plaintext dezelfde zijn, met $IC = 1$ voor een random tekst waarbij elke letter evenveel voorkomt. Voor een Engelse tekst ligt de IC rond de 1.73. Merk op dat bij deze waarde geen rekening gehouden wordt met welke frequentie bij welke letter hoort. Dit betekent dat een plaintext na een monoalfabetische substitutie zijn IC behoudt. Bij een Vigenère ciphertekst met sleutellengte n wordt op elke letter dezelfde monoalfabetische substitutie toegepast als op elke letter er op kn posities vandaan (k geheel). Als we een sleutellengte gokken, kunnen we de tekst verdelen in verzamelingen letters die met dezelfde substitutie versleuteld zouden zijn. Indien de gegokte lengte correct is, moet (indien de ciphertekst lang genoeg was) elke verzameling een redelijk hoge IC hebben, en moeten deze waarden redelijk dicht bij elkaar liggen. Indien de gegokte lengte fout is, zijn de letters in een verzameling niet met dezelfde monoalfabetische substitutie versleuteld (tenzij de gegokte lengte een veelvoud van de correcte is) en lijkt dit eerder een willekeurige verzameling letters, wat een IC dicht bij 1 zal opleveren.

Voor onze ciphertekst konden we dus alle mogelijke kolomtransposities ongedaan maken tot een bepaald aantal kolommen om dan te controleren of een mogelijke Vigenère sleutellengte een hoge IC opleverde. Voor een ciphertekst waarop een enkele kolomtranspositie toegepast is met $k \in [1, n]$ kolommen, zijn $\sum_{k=1}^n k!$ transposities mogelijk. Dit wordt al snel onmogelijk om in een haalbare tijd uit te rekenen, maar gelukkig is het aantal kolommen doorgaans klein.

Het ongedaan maken van de transposities gebeurt voor elke mogelijke permutatie van k kolommen als volgt: de ciphertekst lengte l bestaat uit opeenvolgend de letters uit kolommen 1 t.e.m. k . In elke kolom komen minstens $\lfloor \frac{l}{k} \rfloor$ voor. In de eerste $l \% k$ kolommen (in de volgorde bepaald door het code-

woord voor de kolomtranspositie = gepermuteerde kolommen) komt nog 1 extra letter voor, zodat alle kolommen samen uiteindelijk l letters bevatten. We kunnen de kolommen makkelijk opvullen door gewoon de ciphertekst te overlopen en 1 voor 1 de kolommen op te vullen. Daarna overlopen we de kolommen round-robin in gepermuteerde volgorde en halen we telkens de eerstvolgende letter uit de kolom. In deze volgorde vormen de letters de ciphertekst voor de kolomtranspositie. Op elk van deze cipherteksten voeren we dan, voor elke mogelijke sleutellengte l tot een bepaalde waarde, de volgende Vigenèretest uit: we verdelen de ciphertekst in l groepen door de letters 1 voor 1 round-robin over de groepen te verdelen. Elk van deze groepen zou dan door dezelfde monoalfabetische substitutie versleuteld zijn. We berekenen de IC van elke groep en dan het gemiddelde ervan. Indien dit gemiddelde boven een vooraf ingestelde waarde komt, is dit waarschijnlijk de correctie sleutellengte (of een veelvoud ervan).

Bij het toepassen van dit principe bij de gegeven ciphertekst, moesten we eerst wat spelen met de variabelen (maximale keylengtes voor Vigenère en kolomtranspositie en minimale IC), maar uiteindelijk vonden we (met een runtime van slechts een viertal seconden) zes kolomtransposities van zes kolommen waarbij Vigenère met sleutellengte 8 een IC van ongeveer 2.15 opleverde. Na vergelijken met wat andere zelf berekende IC's van Nederlandstalige teksten, waren we hier al redelijk zeker dat deze plaintekst Nederlands was.

1.3 Vigenere oplossen

Daarna berekenden we bij elk van de zes mogelijke transposities voor elk van de 8 groepen letters de meest voorkomende letter. Aannemend dat dit de E was (in het Nederlands erg waarschijnlijk) konden we meteen de monoalfabetische substitutie ongedaan maken op elke groep. Door de volgorde van de letters te reconstrueren, bekwamen we bij een van de zes transposities de volgende plaintekst, een fragment uit "Erik of het Klein Insectenboek" door Godfried Bomans.

2 Playfair

2.1 De opdracht

De tweede ciphertekst was versleuteld met Playfair. We moesten dus de key zien te vinden waarmee een matrix was opgesteld om digrammen te versleutelen. We hadden op dit punt al een Nederlandse en een Franse tekst ontcijferd, dus we gingen ervanuit dat dit Engels was. Het oplossen van Playfair bleek moeilijker als ADFGVX en Vigenere, na 4 gefaalde pogingen is het ons uiteindelijk gelukt.

2.2 Posing 1: frequentie analyse

Onze eerste poging bestond uit een frequentieanalyse van de digrammen. We vergeleken die waarden met gekende waarden voor digrammen in het Engels die we zelf hadden berekend aan de hand van enkele Engelse plain-teksten. Na veel puzzelwerk raakten we echter niet erg ver. Er zijn 600 digrammen in Playfair (hoewel ze niet allemaal in de ciphertekst voorkwamen) en door dicht bij elkaar gelegen frequenties was het bijna onmogelijk ze juist te kiezen. We bekeken ook de frequenties van opeenvolgende digrammen samen en we hielden rekening met frequente digrammen waarvan ook het omgekeerde frequent was.

2.3 Posing 2: slimme frequentie analyse

Aangezien we door gewoon naar de frequenties te kijken toch 2 digrammen vrij zeker wisten ("OS" \leftrightarrow "th", "OB" \leftrightarrow "he"), probeerden we om gebruik te maken van de structuur van het Playfair vierkant¹. Dit werkte echter ook niet, omdat we geen van de andere digrammen echt zeker wisten, en diegenen die we dachten juist te gokken bleken niet in het vierkant te passen.

Dus probeerden we de ciphertekst te bruteforcen met keys waarbij deze reeds gevonden digrammen klopten, maar vonden ook zo het antwoord niet.

2.4 Posing 3: Hill Climb Algoritme

Daarna gooiden we het over een andere boeg en gingen we op zoek naar een algoritme om de ciphertekst volledig geautomatiseerd te kraken. Eerst maakten we een implementatie van een hill climb algoritme. We starten met een bepaalde startset van mogelijke keys (in ons geval 100 random gekozen keys), de besten op basis van Index of Coincidence²³ hieruit te kiezen en deze te combineren, en deze combinaties dan terug als nieuwe startset te beschouwen. Op een gegeven moment zitten we in een maximum (lokaal) en dit wordt dan teruggegeven. Doordat we voor de combinatie-stap kozen voor een groot aantal keer 2 letters in een key te wisselen en er dus eigenlijk geen combinatie plaatsvond duurde dit algoritme extreem lang om iets te vinden of belande het direct in een lokaal en zeer slecht maximum.

¹<http://www.umich.edu/~umich/fm-34-40-2/ch7.pdf>

²<http://practicalcryptography.com/cryptanalysis/text-characterisation/index-coincidence/>

³http://en.wikipedia.org/wiki/Index_of_coincidence

2.5 Posing 4: Churn Algoritme

Daarna stootten we op het zogenaamde Churn algoritme ⁴ ⁵. Dit algoritme is gelijkaardig aan simulated annealing, alleen heel wat simpeler om te implementeren.

Elke plaintekst krijgt een score toegewezen als volgt: voor elke mogelijke digram in het Engels werd de frequentie geanalyseerd. Hiervan werden telkens de log genomen om de invloed van erg grote waarden te beperken, en werden deze waarden herschaald naar 0-9. Nu wordt voor elk digram (ook twee opeenvolgende letters die volgens Playfair in verschillende digrams zitten!) in de plaintekst de frequentie van 0-9 bij de score van de plaintekst geteld. Hoe hoger de score, hoe waarschijnlijker dat de tekst Engels is dus. Merk hierbij op dat de plainteksten van de gegeven ciphertekst komen, dus erg hoog scorende maar niet-Engelse plainteksten als "eeeeeeeeee" zullen niet voorkomen. In het algoritme starten we met een zogenaamde parent key (bv. gewoon het alfabet) waarmee we de ciphertekst ontcijferen en een score toekennen. Daarna voeren we een kleine verandering door aan de parent key en noemen we het resultaat de child key. Deze verandering kan een horizontale of verticale spiegeling, een combinatie van de twee, een verwisseling van twee willekeurige rijen of kolommen of een verwisseling van twee letters zijn. Hierbij komt de verwisseling van twee letters veel meer voor dan de andere opties, dit omdat er veel meer mogelijke verwisselingen van twee letters zijn. De plaintekst voor de child key wordt ook geëvalueerd. Indien de child key beter scoorde, vervangt deze de parent key. Indien de parent key beter scoorde, wordt een willekeurig getal uit een array van 100 getallen gekozen. Indien het verschil tussen parent en child key scores minder was dan dit gekozen getal, vervangt de child key toch de parent key. Hierdoor kan het algoritme uit lokale maxima raken. Het algoritme blijft oneindig lopen en print de uitkomst van een iteratie enkel indien een nieuwe topscore bereikt is. Merk op dat de 100 getallen in de genoemde array zodanig gekozen zijn dat de kans dat child parent vervangt, gelijkaardig is aan die bij simulated annealing. Bij sommige runs van het algoritme vonden we al na een tweeduizendtal iteraties een tekst die heel erg op Engels leek. Het antwoord was niet helemaal correct gezien bij de logaritmen van de frequenties van digrammen geen rekening gehouden werd met de meer voorkomende X bij Playfair. Het was wel dicht genoeg bij Engels dat we de laatste aanpassingen handmatig konden doorvoeren. We vonden als key "A brief history of time", met als plaintekst het begin van "A Brief History of Time: From the Big Bang to Black Holes" door Stephen Hawking. Het

⁴<http://www.cryptoden.com/index.php/algorithms/churn-algorithm/>
20-churn-algorithm

⁵<http://s13.zetaboards.com/Crypto/topic/6781204/1/>

bijbehorende vierkant kan u vinden in Figure 1 ⁶. Merk op dat we de twee lijsten met waarden op <http://www.cryptoden.com/> vonden, maar de code verder helemaal zelf geschreven is en enkel gebaseerd is op de beschrijving van het algoritme.

Volgens de beschrijving van het algoritme waren de 100 waarden in de array afgesteld op een ciphertekst van 100-120 karakters en moest deze nog geschaald worden voor langere teksten. Wij kregen echter betere resultaten zonder de waarden te schalen.

Het algoritme in `playfair.py` is een licht aangepaste versie van wat we eerst gebruikten. Het geeft vaker snel een antwoord door rollbacks uit te voeren als een tijdje geen vooruitgang geboekt wordt, of zelfs helemaal opnieuw te beginnen. Ook is het scoren nu aangepast aan de X'en in Playfair waardoor exact de correcte plaintekst wordt gevonden. De gevonden key matrix is niet altijd de matrix gegenereerd met "abriefhistoryoftime", maar wel altijd een correcte matrix. Gezien niet alle digrammen voorkomen, zijn meerdere correcte matrices mogelijk.

In de eerste twee lijntjes van het Churn algoritme wordt een vaste seed ingesteld. Deze levert al na 2406 iteraties het antwoord op. Om met een andere seed te proberen, moeten de eerste twee regels code verwijderd worden. Hierdoor kan het algoritme wel langer duren. De variërende runtime is een gevolg van de niet-deterministische aard van het algoritme. Gezien de code niet concurrent is, is het aangewezen om het programma meerdere keren tegelijk te draaien om sneller tot een resultaat te komen.

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

Figure 1: The playfair square with key A brief history of time

3 ADFGVX

3.1 De opdracht

Om ADFGVX te kraken moeten we eerst de morse code decoderen, daarna de kolom transpositie ongedaan maken en vervolgens het vierkant vinden om de oorspronkelijke tekst te bekomen.

⁶http://www.fisica.net/relatividade/stephen_hawking_a_brief_history_of_time.pdf#page=3

3.2 Morse decoderen

Dit is snel gedaan door de tekst op te splitsen in de strings die tussen ”/” staan en deze via een simpele map om te zetten naar hun bijbehorende characters.

3.3 De kolomtranspositie

Aangezien ADFGVX eindigt met een enkele kolomtranspositie, moesten we deze eerst ongedaan maken. Hiervoor gebruikten we hetzelfde systeem als beschreven bij Vigenre: voor alle mogelijke transposities tot een bepaald aantal kolommen werd de index of coincidence berekend, waarna die met de hoogte index gekozen werd. Merk op dat we hierbij de digrammen moesten gebruiken om de index te berekenen. Uiteindelijk vonden we 4 mogelijke kolomtransposities met 4 kolommen, met elk een even grote IC.

3.4 Vinden van de taal.

Door eerst een frequentieanalyse te doen op de 4 meest waarschijnlijke teksten, kregen we de onderstaande tabel.

'FV'	16.93	'AA'	8.26	'DX'	8.02	'AD'	7.80
'XV'	7.32	'VD'	7.18	'AF'	6.15	'FF'	5.80
'GG'	5.64	'DD'	4.91	'XD'	3.64	'XG'	3.18
'FA'	3.10	'DG'	2.94	'VX'	1.59	'DF'	1.21
'VA'	1.16	'VG'	1.16	'GF'	0.99	'GD'	0.67
'AV'	0.56	'GX'	0.51	'FG'	0.32	'XX'	0.13
'AG'	0.13	'VV'	0.10	'FD'	0.08	'XF'	0.08
'FX'	0.05	'XA'	0.05	'DA'	0.05	'VF'	0.05
'DV'	0.05	'AX'	0.02	'GA'	0.0	'GV'	0.0

Om deze tabel te analyseren vergelijken we hem gewoon met gekende frequenties⁷. Dit kan omdat de digrammen in ADFGVX voor enkele characters staan. In ADFGVX kan men ook cijfers gebruiken. Deze staan niet in de frequentietabellen vermeld, maar dit is niet echt een probleem, aangezien deze waarschijnlijk een redelijk kleine frequentie hebben. Dit gaf ons wel een vervormde index of coincidence, waardoor we puur op deze waarde de taal niet konden bepalen. Het viel ons wel op dat het meest voorkomende digram, 'FV' bijna dubbel zo frequent was als het tweede. Van de waarschijnlijke talen voor deze tekst, zijn het Frans en Duits de enige met dit kenmerk. Aangezien de Enigma code in het Duits is, is het zeer waarschijnlijk dat deze tekst in het Frans is geschreven.

⁷http://en.wikipedia.org/wiki/Letter_frequency

3.5 Vinden van de bron tekst

Voordat we begonnen met letters te vervangen hebben we eerst het aantal mogelijke teksten terug gebracht van 4 naar 2. We hebben dit gedaan door te kijken naar de digrammen die 2 maal op elkaar volgen. Bij twee van de vier mogelijke teksten kwam een opeenvolging van twee keer hetzelfde digram erg veel voor. Gezien dit in het Frans minder voorkomt, konden we deze teksten al elimineren.

Nu we nog 2 mogelijke teksten hadden, hebben we het werk opgesplitst onder Jakob en Robin, die elks een tekst probeerden te kraken.

Door eerst de meest frequente letters in te vullen (FV=e, DX=n, ...) en daarna met trial en error de andere redelijk frequente characters in te vullen, verschenen er Franse woorden, of strings die erg leken op een Frans woord, hierdoor konden we ook de minder frequente letters invullen. Eens ongeveer de helft van de digrammen was vervangen door een character, konden we zinnen lezen en zo de andere characters aanvullen, eens we de eerste zin zeker wisten konden we Google aanspreken ⁸ en vonden we dat het ging om het eerste hoofdstuk van "*Vingt mille lieues sous les mers*" van Jules Verne.

Zoals reeds vermeld hadden we 2 teksten opgelost, beide gaven dezelfde tekst. Als we kijken naar de vierkanten die beiden gaven (Figure 2 en 3), zien we dat de ene de getransponeerde versie van de andere is. Dit betekent dat de digrammen voor de ene versie de omgekeerde zijn van de andere versie. Ene ene ciphertekst is dus gelijk aan de andere ciphertekst met elk digram omgedraaid, voor de kolomtranspositie. Gezien de kolomtranspositie met een even aantal kolommen gebeurde, kan door een verschillende kolomtranspositie toe te passen op beide teksten, dezelfde uiteindelijke ciphertekst bekomen worden.

	A	D	F	G	V	X
A	a	5	c	?	q	w
D	s	o	2	x	i	d
F	r	g	l	b	0	1
G	6	m	y	u	f	p
V	h	3	e	?	z	t
X	4	n	8	j	v	k

Figure 2: Vierkant van de 1e tekst

	A	D	F	G	V	X
A	a	s	r	6	h	4
D	5	o	g	m	3	n
F	c	2	i	y	e	8
G	?	x	b	u	?	j
V	q	l	0	f	z	v
X	w	d	1	p	t	k

Figure 3: Vierkant van de 2e tekst

⁸https://www.google.be/search?q=1%27annee+1966+fut+marquee+par+une+evenement&oq=1%27annee+1966+fut+marquee+par+une+evenement&aqs=chrome..69i57.1740j0j7&sourceid=chrome&es_sm=122&ie=UTF-8#q=1%27annee+1966+fut+marquee+par+un+evenement+bizarre

4 Enigma

4.1 Opdracht

De vierde ciphertekst was versleuteld met Enigma. Eerst implementeerden we een volledige Enigma machine. Daarna gingen we op zoek naar de gebruikte rotoren en hun beginstand.

4.2 Een beetje extra onderzoek

Voor we aan het kraken van enigma begonnen hebben we eerst het internet nog gebruikt om wat extra informatie te verzamelen. Deze info en de nota's van de les stelden ons in staat om de tekst relatief eenvoudig te kraken. Hieronder een korte oplistng met de belangrijkste bronnen van informatie die we gebruikten om meer te leren over Enigma, de geschiedenis en het kraken.

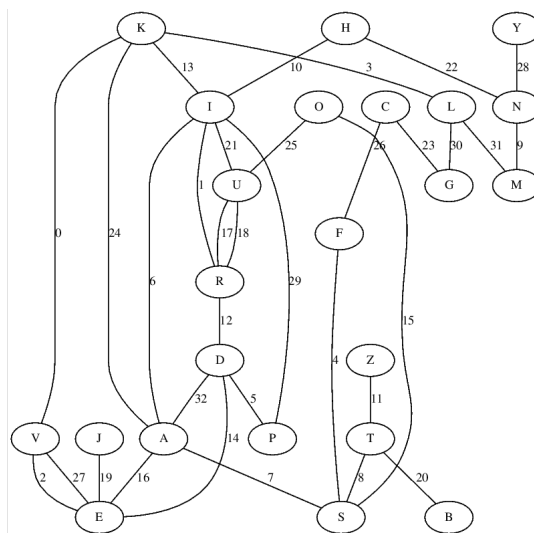
- 2 videos van Numberphile op Youtube over enigma:
 - https://www.youtube.com/watch?v=G2_Q9FoD-oQ
Een video over de werking van Enigma, de internals, het elektrisch circuit ed.
 - <https://www.youtube.com/watch?v=V4V2bpZlqx8>
Een video over hoe de Engelsen de code konden kraken. Deze was niet echt van nut voor het kraken dat wij moesten doen, omdat wij reeds een Crib gekregen hadden, dit gaat meer over hoe de engelsen zon crib konden vinden.
- 2 Videos van Computerphile over Bletchley park en Enigma
 - https://www.youtube.com/watch?v=d2NWPG2gB_A https://www.youtube.com/watch?v=kj_7Jc1mS9k Een iets meer in depth gesprek over de geschiedenis van Enigma en de handelingen in Bletchley park.
- De wikipedia pagina's over Enigma en Alan Turing
 - http://en.wikipedia.org/wiki/Alan_Turing
 - http://en.wikipedia.org/wiki/Enigma_machine
- <http://www.bletchleypark.org.uk/content/hist/>
De Pagina van Bletchley Park met een heel stuk geschiedenis rond Enigma.

4.3 Maken van de Enigma machine

Eerste stap om enigma te kunnen ontcijferen was om een werkende enigma machine te maken. Als taal kozen we voor Go, omdat deze het heel eenvoudig maakt om concurrent functies uit te voeren. Op deze manier zouden we alle rotor posities tegelijk kunnen proberen, net als "The Bombe" dit deed in wereldoorlog II. De implementatie was niet zo moeilijk, met de info die we hadden uit de les, konden we eenvoudig de verschillende componenten implementeren: Rotor, Reflector en Plugboard. Voor elk van deze componenten schreven we testen zodat we zeker waren dat er geen fouten inzaten voor we ze samenbrachten in de Enigma klasse. Deze zorgde voor het linken van de componenten: gaf character per character aan de componenten en concateneerde de ze terug tot de geëncrypteerde of decrypteerde tekst. Om de volledige machine eenvoudig te kunnen gebruiken hebben we een JSON parser toegevoegd die een JSON file neemt en uit de info in deze file een enigma construeert. Een voorbeeld file kan u vinden in de appendix. Om de machine te testen encrypteerden we enkele teksten via de webapp⁹ die de professor ons had bezorgd en lieten ze dan door onze machine decoderen.

4.4 Crib graph en begin positie van de rotors

Er was een crib gegeven, dus we konden makkelijk een crib graph opstellen. Hiervoor stelden we manueel een .dot file om, waarmee we een visuele voorstelling genereerden. Deze is hieronder weergegeven.



Aan de hand van de graph konden we op zoek naar gesloten paden. Door de lengte van de crib waren er heel wat mogelijkheden. We bepaalden voor de

⁹<http://www.algebra.ua.ac.be/stijn/enigma.phtml>

letter U 6 gesloten paden. We gingen dan, met elke mogelijke volgorde van rotoren, op zoek naar een k waarvoor een letter invariant bleef op elk van die paden. Hiervoor was een kleine modificatie aan onze geïmplementeerde Engima machine voldoende. We vonden dat er hiervoor slechts één optie was, namelijk rotorvolgorde 420 met als beginstand KSY. De invariante letter was hier de U, wat betekent dat de U door het plugboard niet aangepast wordt. We herhaalden deze test met de letters A, D en I, waarvoor we ook telkens 5 à 6 gesloten paden zochten. Hier vonden we ook telkens slechts 1 of 2 resultaten, waaronder altijd **rotorvolgorde 420 met beginstand KSY**. Dit was dus zeker het juiste antwoord. Uit deze resultaten vonden we ook dat het plugboard I en Y verwisselt, en de A en de D niet aanpast. Nu moesten we enkel nog op zoek naar de rest van het plugboard.

4.5 Bepalen van het plugboard en ontcijferen van de tekst

Omdat we een behoorlijk grote crib hadden, waren er voor de meeste letters gesloten paden te vinden in de graph. We konden dus gewoon een versimpelde versie van de voorgaande code draaien voor elke letter met gesloten paden om het plugboard verder te bepalen. Hiervoor hoefden we de test enkel voor de correcte rotorvolgorde en beginstand draaien. De enige letters zonder gesloten paden waren B, J, Q, T, W, X, Y en Z waarbij Q, W en X helemaal niet in de graph voorkwamen, en we al wisten dat Y met I werd omgewisseld. We gingen dus enkel de mappings van de letters met gesloten paden zoeken. Hierdoor vonden we ook de mappings voor B, Q, W en Z omdat ze elk verwisseld werden met een letter die wel gesloten paden had. We hadden het plugboard dus op J, T en X na bepaald. Er waren nu echter maar 4 mogelijke plugboards over: ofwel werden twee van de drie letters met elkaar gewisseld ofwel werd geen enkele gewisseld. Door de ciphertekst met elk van de vier opties te decipheren, vonden we dat enkel die waarbij J, T en X niet werden aangepast de crib juist ontcijferde en dus juist was. Hiermee hadden we ook het plugboard volledig bepaald en konden we de tekst volledig ontcijferen. Het was een deel uit *Die Blechtrommel* van Günter Grass¹⁰.

Appendices

A Oplossingen

De teksten die we vonden na het decoderen

¹⁰<http://www.lawrenceglatz.com/germ3230/texte/grass1.htm>

A.1 Vigenère

DEKLEINEERIKLAGJUISTOPHETOGENBLIKDATDITBOEKJEBEGINTINHETOUBE
DVANGROOTMOEDERPINKSTERBLOMMETDETROONHEMELENDEZIJDENKWASTE
NENKEEKOVERDERANDVANHETBLANKELAKENDESCHEMERIGEKAMERINHETWA
SHETUURWAAROPDEKLEINEMENSENNAARBEDGAANHETUURWAARDEGROTEME
NSENNIETVANWETENALLEVERTROUWDEDEDINGENVANDEMUURVERVAGENZOETJ
ESAANINHETGROEIENDEDUISTERENDEWERELDWORDTSTILZOSTILDATZIJZELFS
NIETMEERADEMTBUITENSTAPNOGIEMANDVOORBIJSTAPSTAPZOKLINKTHETEN
INDEVERTEROEPTTEENJONGETJEHOOGENFIJNNAAREENANDERJONGETJEZIJNST
EMKLINKTINDEAVONDENJEDENKTDAAARISTOCHEENJONGETJEOPDEWERELDDAT
NOGNIETINBEDLIGTERIKLAGSTILTEKIJKENNAARHETRAAMINDEVERTEENNAAR
DESCHEMERENDEPORTRETTENVANDEMUURHETISNETDACHTHIJOERIETSGEBE
URENGAATENMISSCHIENGAATEROOKWELIETSGEBEURENENHIJBESLOOTOMNUE
ENSNIETGELIJKOPANDEREAVONDENINSLAAPTEVALLENMAARGOEDOPTETLETTE
NOFERMISSCHINIETSGEBEURENGINGNUWASDAAREENGOEDMIDDELVOORWAN
TONDERZIJNHOOFDKUSSENLAGREENBOEKJESOLMSBEKNOPTENATUURLIJKEHIST
ORIEGEHETENENERIKMOESTDAARVOORMORGENALLEINSECTENUITKENNENHIJ
HADERDEZEHELEWOENSDAGMIDDAGUITZITTENLERENENWASTOTAANDEMEIKE
VERSGEKOMENMORGENOCHTENDONDERHETSPEELKWARTIERZOUHIJDEMEIKEV
ERSERBIJNEMENLAATEENSKIJKENMOMPELDEERIKHOEVEELPOTENHEEFTEENW
ESPOOKALWEERZESDEOGENZIJNAPARTVERSTELBAARENSTAANVOORINDEKOPM
OOIZIJLEVENNIETINKORVENGELIJKDEBIJENMAARJAWAARLEVENZIJDANZIJZULL
ENAPARTLEVENDENKIKNUDATDOETEROOKNIETTOEZIJBEHORENTOTDEFAMILIE
DERVLIESVLEUGELIGENENHEBBENGEKNIKTESPRIETENENHOESTAATHETMETDE
VLINDERS

A.2 ADFGVX

LANNEE1866FUTMARQUEEPARUNEVENEMENTBIZARREUNPHENOMENEINEXPLIQ
UEETINEXPLICABLEQUEPERSONNENASANSDOUTEOUBLIESANSPARLERDESRUME
URSQUIAGITAIENTLESPOPULATIONSDESPORTSETSUREXCITAIENTLESPRITPUBLI
CALINTERIEURDESCONTINENTSLESGENSEMERFURENTPARTICULIEREMENTEM
USLESNEGOCIANTSARMATEURSCAPITAINESDENAVIRESSKIPPERSETMASTERSDE
LEUROPEETDELAMERIQUEOFFICERSDESMARINESMILITAIRESDETOUSPAYSETAP
RESEUXLESGOUVERNEMENTSDESDIVERSETATSDESDEUXCONTINENTSSEPREOCC
UPERENTDECEFAITAUPLUSHAUTPOINTENEFFETDEPUISQUELQUETEMPSPLUSIEU
RSNAVIRESSETAIENTRENCONTRESSURMERAVECUNECHOSEENORMEUNOBJETLO
NGFUSIFORMEPARFOISPHOSPHORESCENTINFINIMENTPLUSVASTEETPLUSRAPIDE
QUUNEBALEINELESFAITSRELATIFSACETTEAPPARITIONCONSIGNESAUXDIVERSLI
VRESDEBORDSACCORDAIENTASSEZEXACTEMENTSURLASTRUCTUREDELOBJETO
UDELETREENQUESTIONLAVITESSEINOUEDESESMOUVEMENTSLAPUISSANCESURP
RENANTEDESALOCOMOTIONLAVIEPARTICULIEREDONTILSEMBLAITDOUESICETA
ITUNCETACEILSURPASSAITENVOLUMETOUSCEUXQUELASCIENCEAVAITCLASSES

JUSQU'ALORS NICUVIERNIL ACEPEDENIMDUMERILNIMDEQUATREFAGES NEUSSENT
ADMIS L'EXISTENCE DU TELMONSTRE MOINS DE LA VOIR VU CE QUI S'APPELLE VU DE
LEURS PROPRES YEUX DES AVANTS APRENDRE LA MOYENNE DES OBSERVATIONS FAI
TES A DIVERSES REPRISES EN REJETANT LE SEUL EVALUATION STIMIDES QUI ASSIGNAIENT
ACET OBJET UN LONGUEUR DE DEUX CENT S'PIEDS ET EN REPOUSSANT LES OPINIONS
EXAGEREES QUI LE DISAIENT LARGES D'UN MILLE ET LONG DE TROIS ON POUVAIT AFFIR
MER CE PENDANT QUE CET TREPHE NOMENAL DE PASSAIT DE BEAUCOUP TOUTES LE
S DIMENSIONS ADMISES JUSQU'AU CE JOUR PAR LES ICHTYOLOGISTES IL EXISTAIT TOU
TEFOIS OR IL EXISTAIT LE FAIT EN LUI MEME ET AIT PLUS NIABLE ET AVEC CE PENCHA
NT QUI POUSSA AUMER VILLEUX LA CERVELLE HUMAIN EN COMPRENDRE LE MOTIO
N PRODUIT DANS LE MONDE ENTIER PAR CETTES URNATURELLE APPARITION QUAN
TALARE JETERAURANG DES FABLES IL FALLAIT Y RENONCER EN EFFET LE 20 JUILLET 1
866 LE STEAMER GOVERNOR HIGGINSON DE CALCUTTA AND BURNACH STEAM NAVIGA
TION COMPANY AVAIT RENCONTRE CETTE MASSE MOUVANTE A CINQ MILLES DANS LE
ST DES COTES DE LA AUSTRALIE LE CAPITAINE BAKER SE CRUT TOUT D'ABORD EN PRESEN
CE D'UNE CUEILLE INCONNU IL SE DISPOSAIT MEME A EN DETERMINER LA SITUATION EXA
CTE QUAND DEUX COLONNES D'EAU PROJETEES PAR LIN EXPLICABLE OBJET SELANCE
RENT EN SI FLANT A CENT CINQUANTE PIEDS DANS L'AIR DONCAMOINS QUE CETECUEI
L NEFTS OUMISAUX EXPANSIONS INTERMITTENTES DUNGEY SERLEGOVERNOR HIGG
INSON AVAIT AFFAIRE BELE TBIENA QUELQUE MAMMIFERE AQUATIQUE INCONNU JU
SQUE LA QUI REJETAIT PAR SEVENTS DES COLONNES D'EAU MELANGEES D'AIRE ET DE
VAPEUR PAREIL FAIT FUTE GALEMENT OBSERVE LE 23 JUILLET DE LA MEME ANNEE DA
NS LES MERS DU PACIFIQUE PAR LE CRISTOBAL COLON DE EST INDIA AND PACIFIC STEA
M NAVIGATION COMPANY DONC CETACE EXTRAORDINAIRE POUVAIT SETRANSPO
RTER D'UN EN DROIT A UN AUTRE AVEC UNE VELOCITE SURPRENANTE PUIS QUE A TROI
S JOURS D'INTERVALLE LE GOVERNOR HIGGINSON ET LE CRISTOBAL COLON LAVAIENT
OBSERVE EN DEUX POINTS DE LA CARTE SEPARES PAR UNE DISTANCE DE PLUS DE SEPT
CENTS LIEUES MARINES QUINZE JOURS PLUS TARD A DEUX MILLE LIEUES DE LA HELVE
TIE DE LA COMPAGNIE NATIONALE ET LES HANNON DU ROYAL MAIL MARCHANT A CON
TRE BORD DANS CETTE PORTION DE L'ATLANTIQUE COMPRENANT ENTRE LES ETATS UNIS
ET L'EUROPE SE SIGNALERENT RESPECTIVEMENT LE MONSTRE PAR 42°15' DE LATITUDE
NORD ET 60°35' DE LONGITUDE AL OUEST DU MERIDIEN DE GREENICH DANS CETTE OBSE
RVATION SIMULTANEE ON CRUT POUVOIR EVALUER LA LONGUEUR MINIMUM D'UN MAM
MIFERE A PLUS DE TROIS CENT CINQUANTE PIEDS ANGLAIS PUIS QUE LES HANNON ET L
HELVETIA ETAIENT DE DIMENSION INFERIEURE ALI BIEN QU'ILS MESURASSENT CENT
METRES DE LE TRAVERSE A LETAMBOR LES PLUS VASTES BALEINES CELLES QUI FREQU
ENTENT LES PARAGES DES ILES ALOUTIENNES LE KULAMMAKET LUMGULLICK NONT
JAMAIS DEPASSE LA LONGUEUR DE CINQUANTE SIX METRES SIMME ELLES LATTEIGN
ENT CES RAPPORTS ARRIVENT COUPS SUR COUP DENOUVELLES OBSERVATIONS FAITES
A BORD DU TRANSATLANTIQUE LE PEREIRE UN ABORDAGE ENTRE LE NADELALIGNE
INMAN ET LE MONSTRE UN PROCES VERBAL DRESSE PAR LES OFFICIERS DE LA FREGAT
E FRANCAISE LANORMANDIE UN TRESSERIEUX RELEVEMENT OBTENU PAR LETAT MAJ
ORDU COMMODE FITZ JAMES A BORD DU LORD CLYDE EMURENT PROFONDEMENT L
OPINION PUBLIQUE DANS LES PAYS D'HUMEUR LEGERE ON PLAISANTALE PHENOMENE

MAIS LES PAYS GRAVES ET PRATIQUES L'ANGLETERRE L'AMERIQUE L'ALLEMAGNE
SE PREOCCUPENT VIVEMENT

A.3 Playfair

A WE L'X L'KNOW N SCIENTISTS SOME SAY IT WAS BERTRAND RUSSELL X L'ONGE GAVE A P
UBLIC LECTURE ON ASTRONOMY HE DESCRIBED HOW THE EARTH ORBITS AROUND T
HE SUN AND HOW THE SUN IN TURN ORBITS AROUND THE CENTER OF A VAST COLLECT
ION OF STARS CALLED OUR GALAXY AT THE X END OF THE LECTURE ALI T'X TLE OLD L
ADY AT THE BACK OF THE ROOM GOT UP AND SAID WHAT YOU HAVE TOLD US IS RUB
BISH THE WORLD IS REAL XLY A FLAT PLATE SUPPORTED ON THE BACK OF A GIANT X T
ORTOISE THE SCIENTIST GAVE A SUPERIOR SMILE BEFORE REPLYING WHAT IS THE T
ORTOISE STANDING ON YOU'RE EVERY CLEVER YOUNG MAN VERY CLEVER SAID THE OLD
LADY BUT IT'S TURTLES X L' THE WAY DOWN MOST PEOPLE WOULD FIND THE PICTUR
E OF FOUR UNIVERSES AS AN INFINITE TOWER OF TORTOISES RATHER X RIDICULOUS BUT
WHY DO WE THINK WE KNOW BETTER WHAT DO WE KNOW ABOUT THE UNIVERSE A
ND HOW DO WE KNOW IT WHERE DID THE UNIVERSE COME FROM AND WHERE IS IT GOIN
G DID THE UNIVERSE HAVE A BEGINNING AND IF SO WHAT HAPPENED BEFORE THEN
WHAT IS THE NATURE OF TIME WILX LITE EVER COME TO AN END CAN WE GO BACK IN TIM
E RECENT BREAKTHROUGHS IN PHYSICS MADE POSSIBLE IN PART BY FANTASTIC NE
W TECHNOLOGIES X SUGGEST ANSWERS TO SOME OF THESE LONGSTANDING QUEST
IONS X SOME DAY THESE ANSWERS MAY EXEMAS OBVIOUS TO US AS THE EARTH ORB
ITING THE SUN OR PERHAPS AS RIDICULOUS AS A TOWER OF TORTOISES ONLY TIME WH
ATEVER THAT MAY BE WILX L TELX L A LONG AGO AS THREE HUNDRED AND FORTY
BC THE GREX EK PHILOSOPHER ARISTOTLE IN HIS BOOK ON THE HEAVENS WAS ABLE T
O PUT FORWARD TWO GOOD ARGUMENTS FOR BELIEVING THAT THE EARTH WAS
AROUND SPHERICAL RATHER THAN A FLAT PLATE FIRST HE REALIZED THAT ECLIPSES OF T
HE MOON WERE CAUSED BY THE EARTH COMING BETWEEN THE SUN AND THE MOON
ON THE EARTH'S SHADOW ON THE MOON WAS ALWAYS ROUND WHICH WOULD BE T
RUE ONLY IF THE EARTH WAS SPHERICAL IF THE EARTH HAD BEEN A FLAT DISK
THE SHADOW WOULD HAVE BEEN ELONGATED AND ELLIPTICAL UNLESS THE E
CLIPSE ALWAYS OCCURRED AT A TIME WHEN THE SUN WAS DIRECTLY UNDER THE C
ENTER OF THE DISK SECOND THE GREX EK SKNEW FROM THEIR TRAVEL THAT THE N
ORTH STAR APPEARED LOWER IN THE SKY WHEN VIEWED IN THE SOUTH THAN IT DID I
N MORE NORTHERLY REGIONS X SINCE THE NORTH STAR LIES OVER THE NORTH POLE I
T APPEARS TO BE DIRECTLY ABOVE AN OBSERVER AT THE NORTH POLE BUT TO SO
MEONE LOOKING FROM THE EQUATOR IT APPEARS TO LIE JUST AT THE HORIZON
FROM THE DIFFERENCE IN THE APPARENT POSITION OF THE NORTH STAR IN EGYPT
AND GREECE ARISTOTLE EVEN QUOTED AN ESTIMATE THAT THE DISTANCE ARO
UND THE EARTH WAS FOUR HUNDRED THOUSAND STADIA IT IS NOT KNOWN EXACTLY
WHAT LENGTH A STADIUM WAS BUT IT MAY HAVE BEEN ABOUT TWO HUNDRED YAR
DS WHICH WOULD MAKE ARISTOTLE'S ESTIMATE ABOUT TWICE THE CURRENTLY A
CCEPTED FIGURE THE GREX EK SEVEN HAD A THIRD ARGUMENT THAT THE EARTH
MUST BE ROUND FOR WHY ELSE DOES ONE FIRST SEE THE SAILS OF A SHIP COMING OV

ERTHEHORIZONANDONLYLATERSEXETHEHULXLARISTOTLETHOUGHTXTHEXEAR
 THWASXSTATIONARYANDTHATXTTHESUNTHEMOXONTHEPLANETSANDTHESTARS
 MOVEDINCIRCULARORBITSABOUTXTHEXEARHTHEBELIEVEDTHISBECAUSEHEF
 ELTFORMYSTICALREASONSTHATXTHEXEARHTHASTHECENTEROFTHEUNIVERSE
 ANDTHATCIRCULARMOTIONWASTHEMOSTPERFECTXTTHISIDEAWASELABORATE
 DBYPTOLEMYINTHESECONDCENTURYADINTOACOMPLETECOSMOLOGICALMODE
 LTHEXEARHTSTOXODATXTHECENTERSURXROUNDEDBYEIGHTSPHERESTHATCA
 RXRIEDTHEMOXONTHESTARSANDTHEFIVEPLANETSKNOWNATXTTHETIM
 EMERCURYVENUSMARSJUPITERANDSATURNX

A.4 Enigma

Rotorvolgorde: 420

Beginstand: KSY

Plugboard: KEDCHGFYJBLWNZPSRQTUVMXIO

Verwisselingen in plugboard: B-K, C-E, F-H, I-Y, M-W, O-Z, Q-S

VIELSPASSMITDIESERUEBUNGAUFENIGMAZUGEGBENICHBININSASSEINERHEIL
 UNDPFLEGEANSTALTMEINPFLEGERBEOBACHTETMICHLASSTMICHKAUMAUSDEM
 AUGEDENNINDERTURISTEINGUCKLOCHUNDMEINESPFLEGERSAUGEISTVONJENE
 MBRAUNWELCHESMICHDENBLAU AUGIGENNICHTDURCHSCHAUENKANNMEINPFL
 EGERKANNALSOGARNICHTMEINFEINDSEINLIEBGEWONNENHABEICHIHNERZAHL
 EDEMGUCKERHINTERDERTURSOBALDERMEINZIMMERBETRITTBEGEBENHEITEN
 AUSMEINEMLEBENDAMITERMICHTROTZDESIHNHINDERNDENGUCKLOCHESKENN
 ENLERNTDERGUTESCHEINTMEINEERZÄHLUNGENZUSCHATZENDENNSOBALDICH
 HMETWASVORGELOGENHABEZEIGTERMIRUMSICHERKENNTLICHZUGEBENSEINN
 EUESTESKNOTENGEBILDEOBEREINKUNSTLERISTBLEIBEDAHINGESTELLTEINEAU
 SSTELLUNGSEINERKREATIONENWURDEJEDOCHVONDERPRESSEGUTAUFGENOM
 MENWERDENAUCHEINIGEKAUFERHERBEILOCKENERKNOTETORDINAREBINDFAD
 ENDIEERNACHDENBESUCHSSTUNDENINDENZIMMERNSEINERPATIENTENSAMMEL
 TUNDENTWIRRTZUVIELSCHICHTIGVERKNORPELTENGESPENSTERNTAUCHTDIES
 EDANNINGIPSLASSTSIEERSTARRENUNDSPIESSTSIEMITSTRICKNADELNDIEAUFHO
 LZSOCKELCHENBEFESTIGTSINDOFTSPIELTERMITDEMGEDANKENSEINEWERKEF
 ARBIGZUGESTALTENICHRATEDAVONABWEISEAUFMEINWEISSLACKIERTESMETA
 LLBETTHINUNDBITTEIHN SICHDIESES VOLLKOMMENSTEBETTBUNTBEHALT VORZ
 USTELLENENTSETZTSCHLAGTERDANNSEINEPFLEGERHANDEUBERDEMKOPFZUS
 AMMENVERSUCHTINETWASZUSTARREMGESICHTALLENSCHRECKENGLEICHZEITI
 GAUSDRUCKZUGEBENUNDNIMMTABSTANDVONSEINENFARBIGENPLANENMEINW
 EISSLACKIERTESMETALLENESANSTALTSBETTISTALSOEINMASSSTABMIRISTESSO
 GARMEHRMEINBETTISTDASENDLICHERREICHTEZIELMEINTROSTISTESUNDKONN
 TEMEINGLAUBEWERDENWENN MIRDIEANSTALTSLEITUNGERLAUBTE EINIGEAND
 ERUNGENVORZUNEHMENDASBETTGITTERMOCHEICHERHOHENLASSENDAMITM
 IRNIEMANDMEHRZUNAHETRITTEINMALINDERWOCHEUNTERBRICHTEINBESUCHS
 TAGMEINEZWISCHENWEISSENMETALLSTABENGEFLOCHTENESTILLEDANNKOMM
 ENSIEDIEMICHRETTENWOLLENDENENESSPASSMACHTMICHZULIEBENDIESICHINM

IRSCHATZENACHTENUNDKENNENLERNENMOCHTENWIEBLINDNERVOSWIEUNERZ
OGENSIESINDKRATZENMITIHRENFINGERNAGELSCHERENANMEINEMWEISSLACKI
ERTENBETTGITTERKRITZELNMITIHRENKUGELSCHREIBERNUNDBLAUSTIFTENDE
MLADELANGGEZOGENEUNANSTANDIGESTRICHMANNCHENMEINANWALTSTULPT
JEDESMALSOBALDERMITSEINEMHALLODASZIMMERSPRENGTDENNYLONHUTUBE
RDENLINKENPFOSTENAMFUSSENDEMEINESBETTESSOLANGESEINBESUCHWAHRT
UNDANWALTEWISSENVIELZUERZAHLENRAUBTERMIRDURCHDIESENGEWALTAKT
DASGLEICHGEWICHTUND DIEHEITERKEITNACHDEMMEINEBESUCHERIHREGESCH
ENKEAUFDEMWEISSENMITWACHSTUCHBEZOGENENTISCHCHENUNTERDEMANEM
ONENAQUARELLDEPONIERTHABENNACHDEMESIHNENGELUNGENISTMIRIHREGE
RADELAUFENDENODERGEPLANTENRETTUNGSVERSUCHEZUUNTERBREITENUND
MICH DENSIEUNERMUDLICHRETTENWOLLENVOMHOHENSTANDARDIHRERNACHS
TENLIEBEZUUBERZEUGENFINDENSIEWIEDERSPASSANDEREIGENENEXISTENZUND
VERLASSENMICHDANNKOMMTMEINPFLEGERUMZULUFTENUNDDIEBINDFADEND
ERGESCHENKPACKUNGENEINZUSAMMELNOFTMALSFINDETERNACHDEMLUFTEN
NOCHZEITANMEINEMBETTSITZENDBINDFADENAUF DROSELNDSOLANGESTILLEZU
VERBREITENBISICHDIESTILLEBRUNOUNDBRUNODIESTILLENENNEBRUNOMUNST
ERBERGICHMEINEJETZTMEINENPFLEGERLASSEDASWORTSPIELHINTERMIRKAUF
TEAUFMEINERECHNUNGFUNFHUNDERTBLATTSCHREIBPAPIERBRUNODERUNVER
HEIRATETKINDERLOSISTUNDAUSDEMSAUERLANDSTAMMTWIRDSOLLTEDEVOR
RATNICHTREICHENDIEKLEINESCHREIBWARENHANDLUNGINDERAUCHKINDERSP
IELZEUGVERKAUFTWIRDNOCHEINMALAUFSUCHENUNDMIRDENNOTWENDIGENU
NLINIERTENPLATZFURMEINHOFFENTLICHGENAUESERINNERUNGSVERMOGENBE
SCHAFFENNIEMALSHATTEICHMEINEBESUCHERETWADENANWALTODERKLEPPU
MDIESENDIENSTBITTENKONNENBESORGTEMIRVERORDNETELIEBEHATTEDENFR
EUNDENSICHERVERBOTENETWASSOGEFAHRLICHESWIEUNBESCHRIEBENESPAPI
ERMITZUBRINGENUNDMEINEMUNABLASSIGSILBENAUSSCHIEDENDENGEISTZUMG
EBRAUCHFREIZUGEBENALSICHZUBRUNOSAGTEACHBRUNOWURDESTDUMIRFUNF
HUNDERTBLATTUNSCHULDIGESPAPIERKAUFENANTWORTETE BRUNOZURZIMME
RDECKEBLICKENDUNDSEINENZEIGEFINGEREINENVERGLEICHHERAUSFORDERND
INDIEGLEICHERICHTUNG SCHICKENDSIEMEINENWEISSESPAPIERHERROSKAR

A.5 Diffie Hellman