04. les 4 vigenere

Auteur	Its Academy
Laatst gewijzigd	18 december 2014
Licentie	CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie
Webadres	https://maken.wikiwijs.nl/45955

Inhoudsopgave

Les 4 Vigenère

Inhoud van les 4: Vigenère

4.1 Het idee van Alberti

Aan het einde van de zestiende eeuw hadden de codebrekers hun achterstand op de cryptografen volledig weggewerkt. Het werd dus hoog tijd om iets nieuws te bedenken. De Italiaanse geleerde Leon Battista Alberti uit Florence, die ook de beroemde Trevi-fontein van Rome ontwierp, had al in de tweede helft van de vijftiende eeuw bedacht dat het goed zou zijn om meerdere cijferalfabetten toe te passen. Door tijdens het vercijferen te switchen van het ene op het andere cijferalfabet zou je de cryptoanalisten op een dwaalspoor brengen. In les 7 lees je hoe Alberti bovendien de eerste was die een cijfermachine vervaardigde.

Het idee wordt in onderstaand voorbeeld geïllustreerd:

Klaar alfabet: 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

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

Door om en om de letters uit het ene en dan uit het andere cijferalfabet te kiezen wordt de gewone frequentieanalyse ontregeld. Het woord *samenzwering* wordt dan bijvoorbeeld vercijferd tot RSDUUNNUZHUK, waarbij dezelfde cijferletter verschillende betekenissen heeft.

Alberti's idee was de belangrijkste doorbraak in meer dan duizend jaar. Hij werkte zijn idee niet verder zelf uit maar liet dat over een een groep intellectuelen. Eerst was het Trithemius, een Duitse abt, daarna Giovanni Porta, een Italiaanse onderzoeker en tenslotte Blaise de Vigenère, een in 1523 geboren Franse diplomaat die het idee verder uitwerkte. Het duurde tot 1586 voordat Vigenère zijn idee lanceerde in zijn werk *Traicté de Chiffres* (verhandeling over het geheimschrift). Toevallig was dat ook het jaar waarin Phelippes het geheimschrift van Mary Stuart kraakte.

4.2 Het Vigenère systeem

Het Vigenère-cryptosysteem werd in 1553 bedacht door Giovanni Batista Belaso, maar vernoemd naar Vigenère, die het systeem verbeterde. Belaso gebruikte een tabel bestaande uit 26 schuifsystemen volgens het Caesarmodel met op de 26e rij het klare alfabet. We noemen dit het Vigenère vierkant.

het Vigenère vierkant
kn.nu/ww.7a2f61d (xls, maken.wikiwijs.nl)

Belaso voegde vervolgens aan het systeem een *sleutelwoord* toe, de feitelijke sleutel van het systeem. Dit sleutelwoord schreef hij boven de klare tekst en herhaalde dat steeds tot het einde van de tekst. De letters van het sleutelwoord bepaalden vervolgens welke rij gebruikt zou moeten worden om de klare letter te versleutelen.

Bijvoorbeeld: het sleutelwoord is VRIENDSCHAP. De tekst is *lieve schat ik houd van jou*.

sleutelwoord:V R I E N D S C H A P V R I E N D S C H A P
klare tekst: l i e v e s c h a t i k h o u d v a n j o u

code tekst: 11 08 04 21 04 18 02 07 00 19 08 10 07 14 20 03 21 00 13 09 14 20
sleutelcode: 21 17 08 04 13 03 18 02 07 00 15 21 17 08 04 13 03 18 02 07 00 15
somrij: 06 25 12 25 17 21 20 09 07 19 23 05 24 22 24 16 24 18 15 16 14 09
cijfertekst: G Z M Z R V U J H T X F Y W Y Q Y S P Q O J

De cijfertekst is dus GZMZR VUJHT XFYWY QYSPQ OJ.
Hierbij volgen we de afspraak om de cijfertekst weer te geven in groepjes van 5 letters. Het voordeel daarvan is dat de zinsstructuur niet langer herkenbaar is, wat het voor de codebreker nog moeilijker maakt.

Afspraak:
De cijfertekst wordt weergegeven in groepjes van 5 (hoofd)letters zonder leestekens.

Opgave 1

a) Gebruik het Vigenère vierkant om de zin '*cryptografie is cool*' te vercijferen volgens het Vigenère-systeem met het codewoord AUDI.

het Vigenère vierkant
kn.nu/ww.e11a388 (xls, maken.wikiwijs.nl)

b) In het codewoord zit een A die dus eigenlijk niets met de klare letters doet. Maakt dit het codewoord zwakker?

4.3 De Vigenère tool

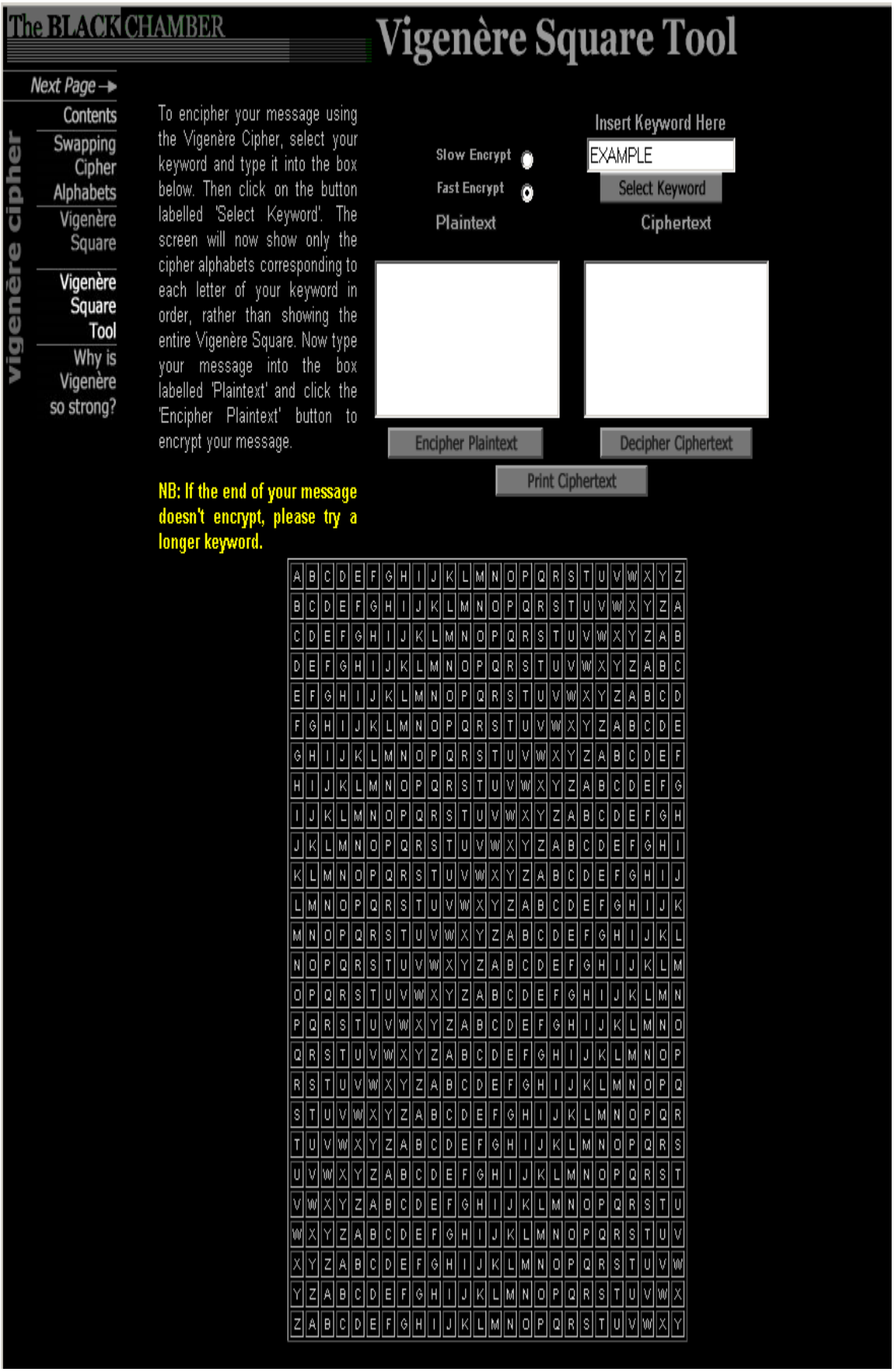
Activiteit

Versleutelen met de CD-rom

Je hebt al snel in de gaten dat het vercijferen op deze manier een hoop tijd kost. Tegenwoordig is het eenvoudig om een computerprogramma te schrijven dat je helpt om de code te vercijferen.
Gebruik onderstaande pagina of, wat beter is, navigeer op de CD-rom van Simon Singh naar Highlights/Viginère tool voor een duidelijke demonstratie.
Neem het *keyword* ***GEHEIM*** en de klare tekst: ***Vigenere stond bekend als le chiffre indechiffrable***.
Letter voor letter levert de tool in de demonstratie op de CD-rom de *ciphertext*. Bekijk aan de linkerkant goed hoe de tool scrollt tussen de verschillende schuifsystemen op aangeven van de letters van het sleutelwoord. Helaas ontbreekt op onderstaande pagina de demonstratie. Op de pagina's 'Swapping Cipher Alfabets' en 'Vigenere Square' is wel extra informatie beschikbaar.

Voer het *keyword* ***GEHEIM*** en de klare tekst (*plain text)* ***Vigenere stond bekend als le chiffre indechiffrable*** in en druk op *encipher.*
Zet de snelheid op Slow Encrypt.

De encryptie moet worden BMNIVQXIZXWZJFLOMZJESWTQILPJNDKMUHMONMMJZMHPL



Klik [hier](#)om naar de site te gaan.

 Meerkeuzevraag

Het Vigenère systeem maakt gebruik van 26 schuif-systemen. Is het aantal mogelijke cijferalfabetten groter, gelijk of kleiner dan bij monoalfabetische substitutie?

a. Groter
a. Gelijk
a. Kleiner

Opgave 2

a) Het ontcijferen van een boodschap die vercijferd is met Vigenère is niet zo eenvoudig als het ontcijferen van een boodschap die vercijferd is met mono-alfabetische substitutie. Leg uit waarom het zo lastig is.
b) Leg uit dat de sleutel vinden in principe niet moeilijk is, d.w.z. met behulp van computers goed te doen, als je weet hoe lang de sleutel is.
c) Leg uit waarom het toch nog heel lastig is de boodschap
QAGQO XVKFV JGARH XOWVL ERAIN KPRLT NNBAH
TNTAR TTYSF VJGXA GNRBR PTXNT GWHED MQKMX
te ontcijferen, ook al weet je dat hij vercijferd is met Vigenère en een sleutelwoord van lengte 3.

Natuurlijk hoef je geen bestaand woord als sleutel te nemen. Sterker nog, het komt de veiligheid van je systeem niet ten goede wanneer je een bestaand woord of bijvoorbeeld de naam van je geliefde neemt, omdat de sleutelruimte er ernstig door beperkt wordt en de sleutel bovendien makkelijker te raden is.

 Reflectie

Als je een codewoord van vier letters gebruikt is het aantal mogelijke cijferalfabetten niet zo gek groot. Met de hand is het een heel karwei om de tekst dan te kraken maar met een computer is het te doen. Waarom is het kraken van het Vigenère-systeem met een codewoord van vier letters toch lastiger dan een gewoon monoalfabetisch cryptosysteem?

klik hier

4.4 Een zwakke plek

Opgave 3

De boodschap:
'je gele kanariepak ok, als je je duikbril maar meeneemt' wordt vercijferd met Vigenère tot
ESMIW ZYGRL MWKTL FCQEW NXKNP YIOOM MWRQL VFSIP JSKQE
Achterhaal het sleutelwoord. Leg duidelijk uit hoe je dit hebt aangepakt. Maak gebruik van deVigenère tabel.

Vigenère tabel
kn.nu/ww.f84f6c5 (xls, maken.wikiwijs.nl)

Men heeft lang gedacht dat het Vigenère systeem niet te kraken was tot in 1863 de Pruisische legerofficier Friedrich Kasiski een methode ontwikkelde om de sleutellengte te achterhalen. Als je de sleutellengte kent kun je de letters die met hetzelfde schuifsysteem vercijferd zijn eruit lichten, daar

een frequentieanalyse op toepassen en zo de sleutel achterhalen. De Britse wiskundige Charles Babbage had enkele jaren eerder dezelfde methode ontwikkeld, maar had dit niet gepubliceerd.

Het achterhalen van de sleutellengte kan op verschillende manieren. We bekijken eerst een andere methode en de methode van Babbage en Kasiski bespreken we in les 5.
De frequentieanalyse berust op het principe dat in een taal bepaalde letters vaker voorkomen.
De eerste letter van de cijfertekst kan in principe elke letter van het alfabet zijn. Het hangt af van de vraag wat de eerste letter van de klare tekst en de eerste letter van het codewoord is. Hetzelfde geldt voor de tweede letter van de cijfertekst.

Laten we de eerste vijf letters nemen van een cijfertekst die in het voorbeeld '*chinese eetstokjes*' verder wordt gebruikt: DSOEU

De eerste letter van het codewoord is een D. Dit is bepaald door de eerste letter van de klare tekst en de eerste letter van het codewoord. De tweede letter van het codewoord is een S en had net zo goed ook een D kunnen zijn. Dit is bepaald door de tweede letter van het codewoord en de tweede letter van de klare tekst. Het codewoord zal van invloed zijn op de vraag welke cijferletters er worden gevormd. Als het codewoord vijf verschillende letters heeft zullen de 19% E's in de klare tekst op vijf verschillende manieren worden versleuteld. De hoge frequentie van de E's wordt daardoor gespreid over vijf cijferletters. En deze cijferletters ontstaan ook nog uit andere combinaties: de letter E wordt door de codeletter P vercijferd als een T (want E is 4, P is 15 en T is 19). De letter L wordt door de codeletter I óók vercijferd als een T (want L is 11, I is 8 en T is 19).
Eenzelfde redenatie geldt voor alle andere letters waardoor de frequenties van de letters op meerdere manieren worden verdeeld over de cijferletters en de frequenties van de cijferletters minder zullen verschillen dan in de klare tekst. Het maakt wel duidelijk dat het belangrijk is een codewoord uit verschillende letters te kiezen en ook nog willekeurig bepaald.

De gebeurtenis dat de eerste en de tweede letter hetzelfde zijn hangt af van het codewoord en de letters van de klare tekst, maar is onvoorspelbaar. Als alle cijferletters dezelfde frequentie hebben is de kans daarop is 1/26 of 0,038 (3,8%). We verwachten daarom dat 1 op de zesentwintig codeletters hetzelfde zal zijn als de volgende letter. Voor een cijfertekst van bijvoorbeeld 330 letters levert dat 12 of 13 overeenkomsten op.
Hetzelfde gebeurt als we de cijfertekst verder opschuiven onder de originele cijfertekst, maar als we de letter D verder doorschuiven dan zal het ooit een keer voorkomen dat hij terechtkomt onder een letter die ook versleuteld is volgens *hetzelfde schuifsysteem*. Om precies te zijn duurt dat net zo lang als de lengte van het sleutelwoord.
De kans dat de letters *dan* hetzelfde zijn hangt alleen af van de vraag wat de klare letter is:
6,72% van de letters in de klare tekst is een a. De kans dat een *a* weer onder een *a* terechtkomt is 6,72%.
0,11% van de letters in de klare tekst is een x. De kans dat een *x* weer onder een *x* terechtkomt is 0,11%.
De kans dat een *e* onder een *e* terechtkomt is maar liefst 19,06%.


Doordenker

De kans dat een *a* weer onder een *a* terecht komt is 6,72%,

de kans dat een *x* onder een *x* terechtkomt is slechts 0,11%,
maar de kans dat een *e* onder een *e* terechtkomt is maar liefst 19,06%.
Bovendien komt het veel vaker voor dat de letter die verschoven wordt een *e* is, namelijk in 19,06% van de gevallen,
terwijl het maar zelden voorkomt dat het een *x* is die verschoven wordt, namelijk in 0,11% van de gevallen.

Waarom is dat zo?

klik hier

Opgave 4

letter	%	letter	%	letter	%	letter	%
a	6,72	h	2,32	o	5,87	v	2,90
b	1,80	i	6,44	p	1,59	w	1,57
c	1,60	j	1,49	q	0,11	x	0,11
d	5,91	k	2,28	r	6,45	y	0,29
e	19,06	l	3,94	s	4,00	z	1,18
f	0,74	m	2,41	t	6,74		
g	3,14	n	9,41	u	1,93		

a) Laat met behulp van de letterfrequentietabel uit les 3 zien dat de kans dat twee willekeurige letters in een Nederlandse tekst hetzelfde zijn ongeveer gelijk is aan 0,077.
b) In een cijfertekst die vercijferd is met een willekeurig sleutelwoord van 6 letters, dat dus geen bestaand woord hoeft te zijn en meerdere keren dezelfde letter mag bevatten, bekijken we twee letters die niet op 6, 12, 18, ... plaatsen uit elkaar liggen. Wat is de kans dat deze twee letters hetzelfde zijn?
c) Leg uit waarom de kans op twee dezelfde letters groter is als de letters een veelvoud van de sleutellengte uit elkaar staan.

Als je in Vigenère een sleutelwoord hebt van bijv. 6 letters, dan zijn in de cijfertekst de letters op plaats 1, 7, 13, 19, ... met dezelfde sleutel vercijferd. Volgens opgave 4 is de kans dat de letters hetzelfde zijn wanneer je 6, 12, 18, 24, ... plaatsen verschuift ruim 2x zo groot (7,7%) als bij andere verschuivingen.
Hetzelfde geldt voor de letters op plaats 2, 8, 14, 20, ... en voor de letters op plaats 3, 9, 15, 21, ... want ook deze zijn met dezelfde sleutel vercijferd.
IOnder het kopje 'Chinese eetstokjes' verder op deze pagina staat een uitgewerkt voorbeeld, waarin je duidelijk kunt zien dat het verschil opvallend is wanneer je een tekst telkens een letter opschuift en vergelijkt met de oude tekst.

Het resultaat van het onderzoek op de pagina 'Chinese eetstokjes' zie je terug in opgave 5:

Opgave 5

Het resultaat van het onderzoek naar de chinese eetstokjes:

Aantal posities verschoven	1	2	3	4	5	6	7	8
Aantal overeenkomsten	10	9	8	22	11	11	12	22

Je ziet dat de overeenkomsten groter zijn bij 4 posities verschoven en bij 8 posities verschoven.
Welke sleutellengte denk je dat de sleutel heeft die voor de vercijfering in het voorbeeld gebruikt is? Waarom?

Opgave 6

Zoals je gezien hebt, is er een manier om de sleutellengte te achterhalen.
Hoe kun je de sleutel kiezen als je toch Vigenère zou willen gebruiken en een niet al te groot risico wilt lopen dat je bericht ontcijferd wordt?

Chinese eetstokjes

De volgende tekst over belasting op wegwerpeetstokjes in China is vercijferd met Vigenère:
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE TKRVF HLREV LRCPH PCGWM PUJIJ SYIPC SIGBD EPHDP DWMDQ BGITS SVQRX GVSQS PRHVF WHTTC GYEHH RXOOP GBGIK BFLKB DENCP ZGFWI ISQAQ CUHKR JIYSJ AGFSI GHVXQ YMIUR HFGZD WVWQK KGHVQ DJITW FLVAH RUSQQ KZLIW PHAWG WITCP XGZDX GBJEC BPIVG FLCOU WGUUS PRVXQ TIIPN RENGK SWHLR EVLRC KRVFH MECFO MLYVX YSHQK ZMSGB NYDWH OGAHX GFKSW HWSVS HXUGW SMXHW XSUAG FNX

We gaan nu proberen de sleutellengte te achterhalen. Als voorbeeld laten we voor een deel van de eerste regel zien hoe je te werk gaat. Dit laten zien voor de hele tekst kost te veel tijd en voegt niets toe. De uitkomst van analyse op de hele tekst is te zien in de tabel onderaan die we door het

rekenblad laten uitrekenen. Hoe je dit zelf kunt onderzoeken met gebruik van Excel wordt toegelicht in het volgende filmpje.

https://youtu.be/8-Rfd3_5W3U

Onder de cijfertekst schrijf je de cijfertekst nog een keer op. Je verschuift de onderste tekst één plaats naar rechts en telt hoe vaak dezelfde letters boven elkaar staan. Dan verschuif je de onderste tekst nog een plaats naar rechts en telt weer hoe vaak dezelfde letters boven elkaar staan, enz. Al deze uitkomsten van het tellen houd je bij in een tabel. Wanneer het aantal plaatsen dat de onderste tekst verschoven is een veelvoud van de sleutellengte is, zal het aantal keer dat dezelfde letters boven elkaar staan groter zijn.

We lichten het toe met een voorbeeld door een deel van de tekst te verschuiven.
In de tabel staat uiteindelijk het resultaat wanneer je dit toepast op de gehele tekst.

DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
*DSOE UHLRI CSIGH VXQYM IUGLR FGHIP OSVKZ GMVXD
1 positie verschoven, 0 overeenkomsten.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
**DSO EUHLR ICSIG HVXQY MIUGL RFGHI POSVK ZGMVX
2 posities verschoven, 0 overeenkomsten.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
***DS OEUHL RICSI GHVXQ YMIUG LRFGH IPOSV KZGMV
3 posities verschoven, 1 overeenkomst.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
****D SOEUH LRICS IGHVX QYMIU GLRFG HIPOS VKZGM
4 posities verschoven, 1 overeenkomst.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
***** DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG
5 posities verschoven, 1 overeenkomst.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
***** *DSOE UHLRI CSIGH VXQYM IUGLR FGHIP OSVKZ
6 posities verschoven, 0 overeenkomsten.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
***** **DSO EUHLR ICSIG HVXQY MIUGL RFGHI POSVK
7 posities verschoven, 0 overeenkomsten.
DSOEU HLRIC SIGHV XQYMI UGLRF GHIPO SVKZG MVXDE
***** ***DS OEUHL RICSI GHVXQ YMIUG LRFGH IPOSV
8 posities verschoven, 2 overeenkomsten.

Gaan we nu de hele tekst vergelijken met de verschoven tekst, dan vinden we de resultaten met gebruik van een werkblad, die in onderstaande tabel staan.

werkblad
kn.nu/ww.4f604e0 (xls, maken.wikiwijs.nl)

Aantal posities verschoven	1	2	3	4	5	6	7	8
Aantal overeenkomsten	10	9	8	22	11	11	12	22

Je ziet dat de overeenkomsten groter zijn bij 4 posities verschoven en bij 8 posities verschoven.

 Activiteit

Ga nu verder met opgave 5 boven op deze pagina.

4.5 Polyalfabetische substitutie en het autokey systeem

Polyalfabetische substitutie is een verbetering van het Vigenèresysteem. Bij Vigenère wordt eigenlijk een aantal keer het schuifcryptosysteem gebruikt, bij polyalfabetische substitutie is dat een aantal keer een monoalfabetische substitutie die steeds herhaald wordt. Je hebt dan bijvoorbeeld 4 keer een gepermuteerd (=gehusseld) alfabet. Voor de vercijfering van de eerste letter gebruik je de eerste permutatie van het alfabet, voor de tweede letter de tweede permutatie van het alfabet, voor de derde letter de derde permutatie van het alfabet, voor de vierde letter de vierde permutatie van het alfabet, voor de vijfde letter weer de eerste permutatie van het alfabet, voor de zesde letter weer de tweede permutatie van het alfabet, enz.

Opgave 7

Is een boodschap die vercijferd is met de polyalfabetische substitutie veel moeilijker om te ontcijferen dan een boodschap die vercijferd is met Vigenère of valt dat wel mee? Leg je antwoord uit.

Het cryptosysteem dat Vigenère wel beschreef wordt autoclave, autokey of autosleutelsysteem genoemd. Dit systeem lijkt erg veel op het Vigenère systeem. Het verschil is dat dit systeem het sleutelwoord slechts één keer aan het begin van de tekst gebruikt. Daarna gebruikt men in plaats van het sleutelwoord de oorspronkelijke tekst. Doordat nu niet steeds het sleutelwoord herhaald wordt, is het systeem moeilijker te kraken.

Voorbeeld:
We vercijferen hieronder de zin '*autoclave is een verbetering van vigenere*' met behulp van het sleutelwoord 'BETER'.

klare tekst: a u t o c l a v e i s e e n v e r b e t e r i n g v a n v i g e n e r e x q x q
sleutel: B E T E R A U T O C L A V E I S E E N V E R B E T E R I N G V A N V I G E N E R
code tekst: 00 20 19 14 02 11 00 21 04 08 18 04 04 13 21 04 17 01 04 19 04 17 08 13 06 21 00 13 21 08 06 04 13 04 17 04 23 16 23 16
sleutelcode: 01 04 19 04 17 00 20 19 14 02 11 00 21 04 08 18 04 04 13 21 04 17 01 04 19 04 17 08 13 06 21 00 13 21 08 06 04 13 04 17
somrij: 01 24 12 18 19 11 20 14 18 10 03 04 25 17 03 22 21 05 17 14 08 08 09 17 25 25 17 21 08 14 01 04 00 25 25 10 01 03 01 07
cijfertekst: B Y M S T L U O S K D E Z R D W V F R O I I J R Z Z R V I O B E A Z Z K B D B H

Opgave 8

Waarom is dit systeem moeilijker te kraken dan het Vigenèresysteem van Belaso?

 Activiteit

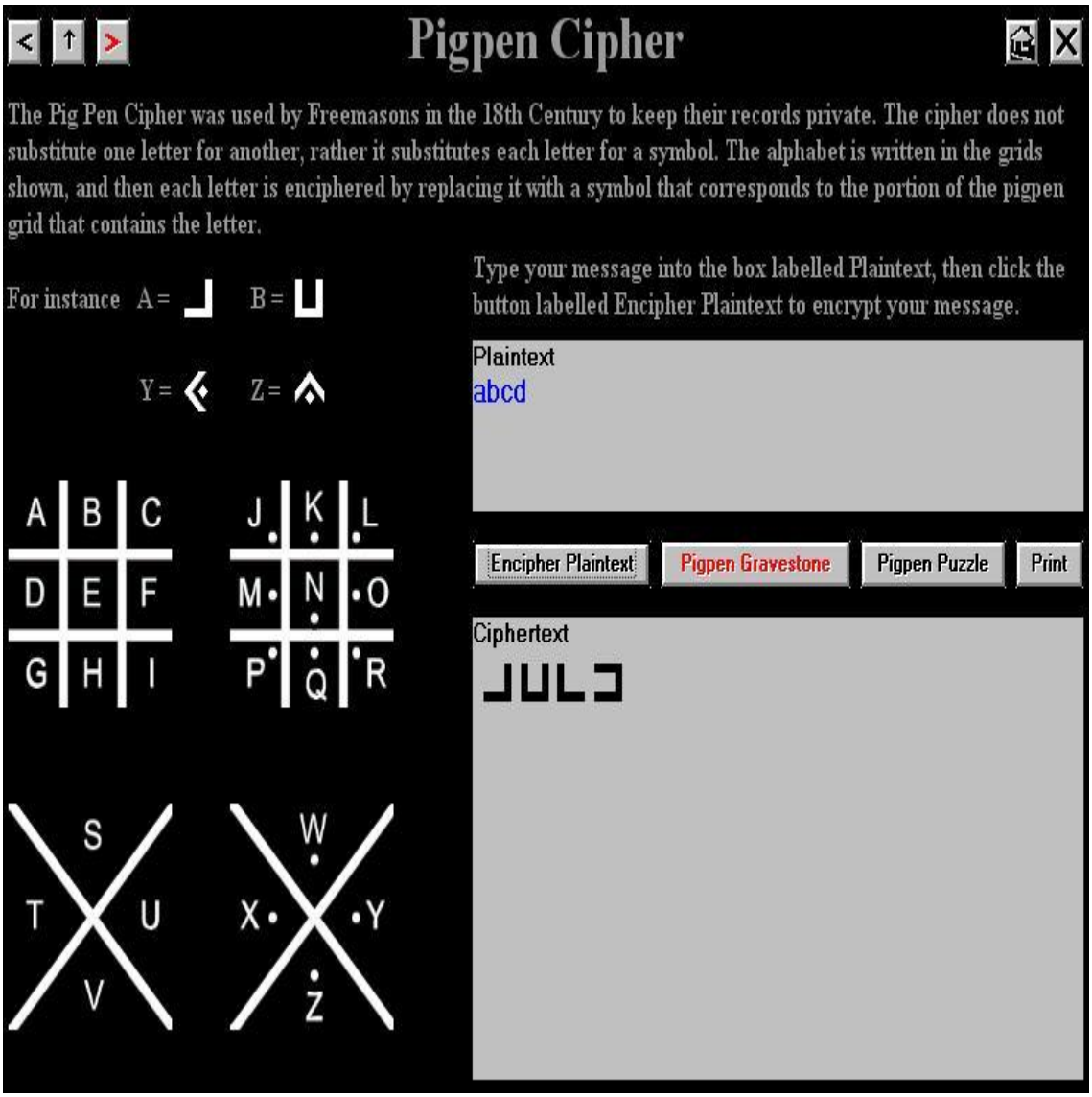
Voor huis-tuin-en-keuken gebruik bleef het monoalfabetische cryptosysteem zelfs in vereenvoudigde vorm nog eeuwen lang in gebruik. Een aardig voorbeeld daarvan is het *varkenshok*-cijfer (zie de sectie 'het varkenshokcijfer'), vroeger gebruikt door vrijmetselaars om hun archieven geheim te houden, maar waarmee tegenwoordig nog alleen kinderen elkaar geheime boodschappen doorsturen.

Lees de screendump onder het kopje '*het varkenshokcijfer' verder op deze pagina* en voer de opdracht

uit.

Het varkenshokcijfer

Hieronder is een screendump te zien van het programma Pigpen Cipher (varkenshokcijfer) van de CD-rom van Simon Singh. Het idee van het varkenshokcijfer is om iedere letter te vervangen door de tekening van het hokje waarin het zit. Lees de Engelse tekst.

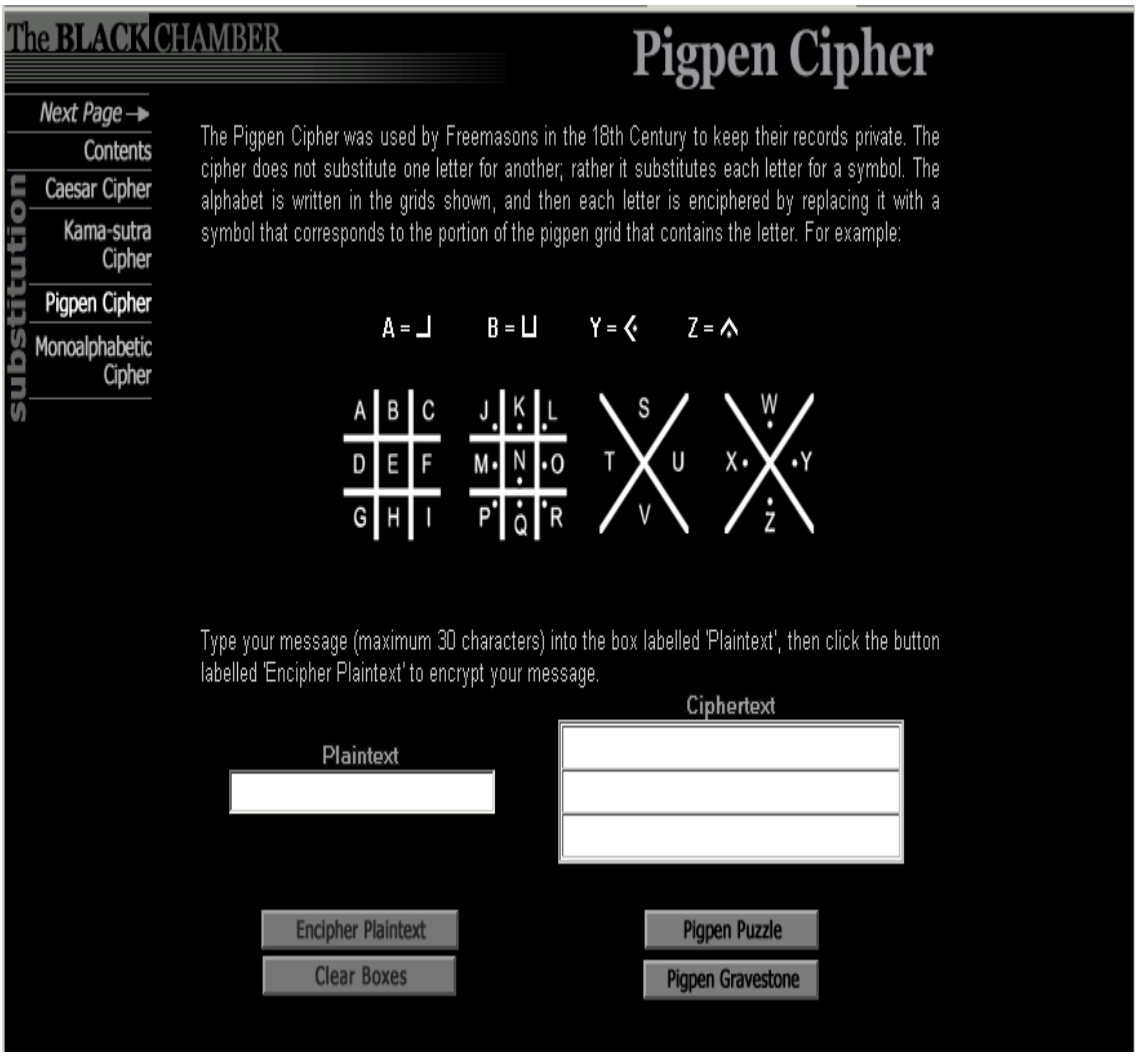


Activiteit

Gebruik de onderstaande pagina, maar bedenk eerst zelf de oplossing in de volgende opdracht:

Wat wordt de cijfertekst bij de invoer van de klare tekst:
'*het wordt weer niks met de elfstedentocht dit jaar*'?

klik hier



klik hier om naar de site te gaan.

 Slotvraag

Waarom is hier sprake van een monoalfabetische substitutie?

klik hier

Het autokey-systeem systeem is ongeveer 200 jaar ongekraakt gebleven. Uiteindelijk heeft Charles Babbage ook dit systeem gekraakt. Als je wilt weten hoe hij dat deed, kun je dat opzoeken op http://en.wikipedia.org/wiki/Autokey_cipher.

Terwijl de behoefte groot was aan een onfeilbaar systeem bleef het systeem toch ongebruikt voor lange tijd. Het waarom is eenvoudig te raden: het was te ingewikkeld. Tegenwoordig is met gebruik van een computer elke tekst eenvoudig om te zetten zoals onze tool laat zien, maar handmatig een tekst versleutelen met voor iedere letter een andere monoalfabetische substitutie is geen pretje. Hetzelfde geldt uiteraard voor het ontcijferen. Daarom werd gezocht naar andere manieren om het monoalfabetische cijfer te verbeteren en te beschermen tegen de frequentieanalyse.

4.6 Het homofone substitutiecijfer

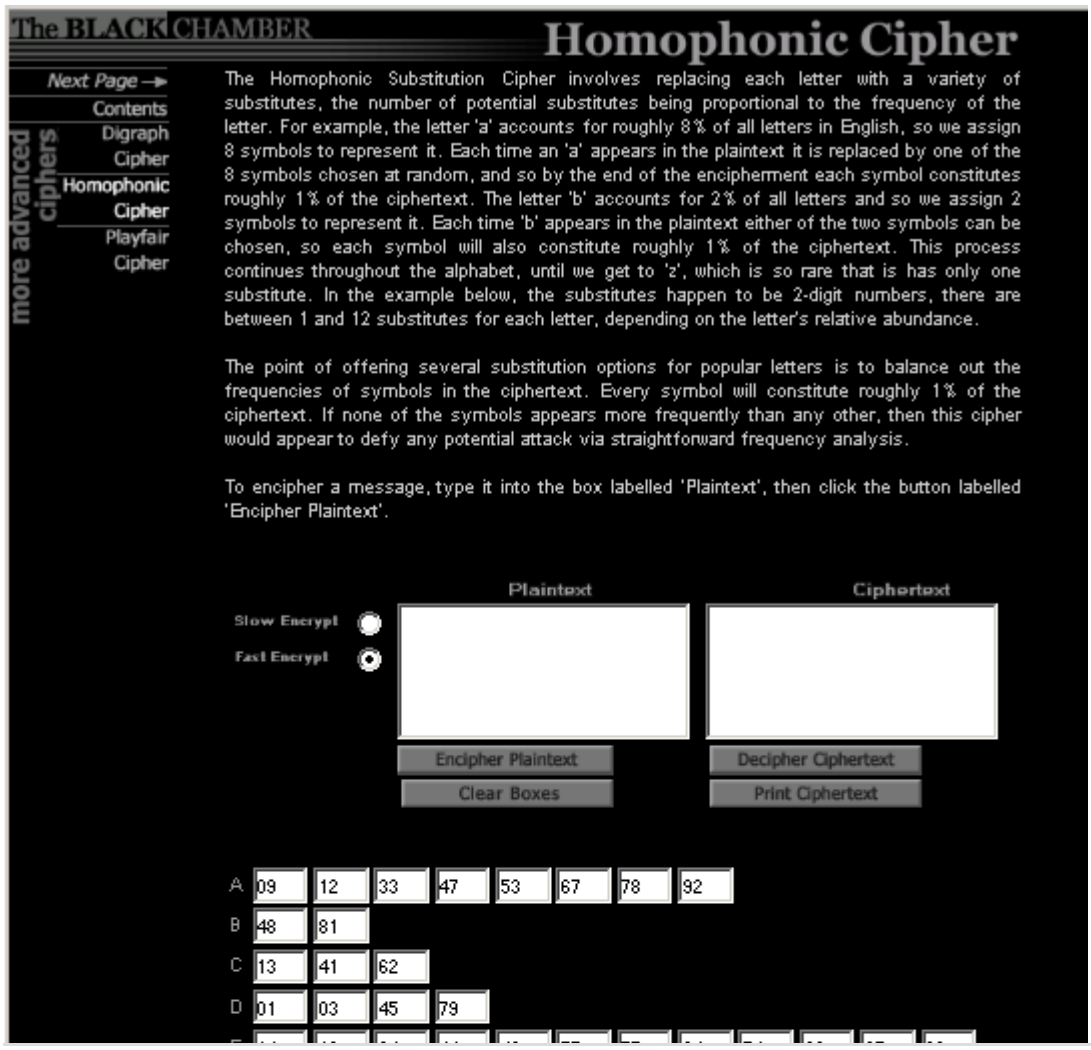
Een goede tussenoplossing die de frequentieanalyse voor grote problemen stelde was het *homofone substitutiecijfer*. Het doel van dit systeem is om de frequenties waarin de letters voorkomen te

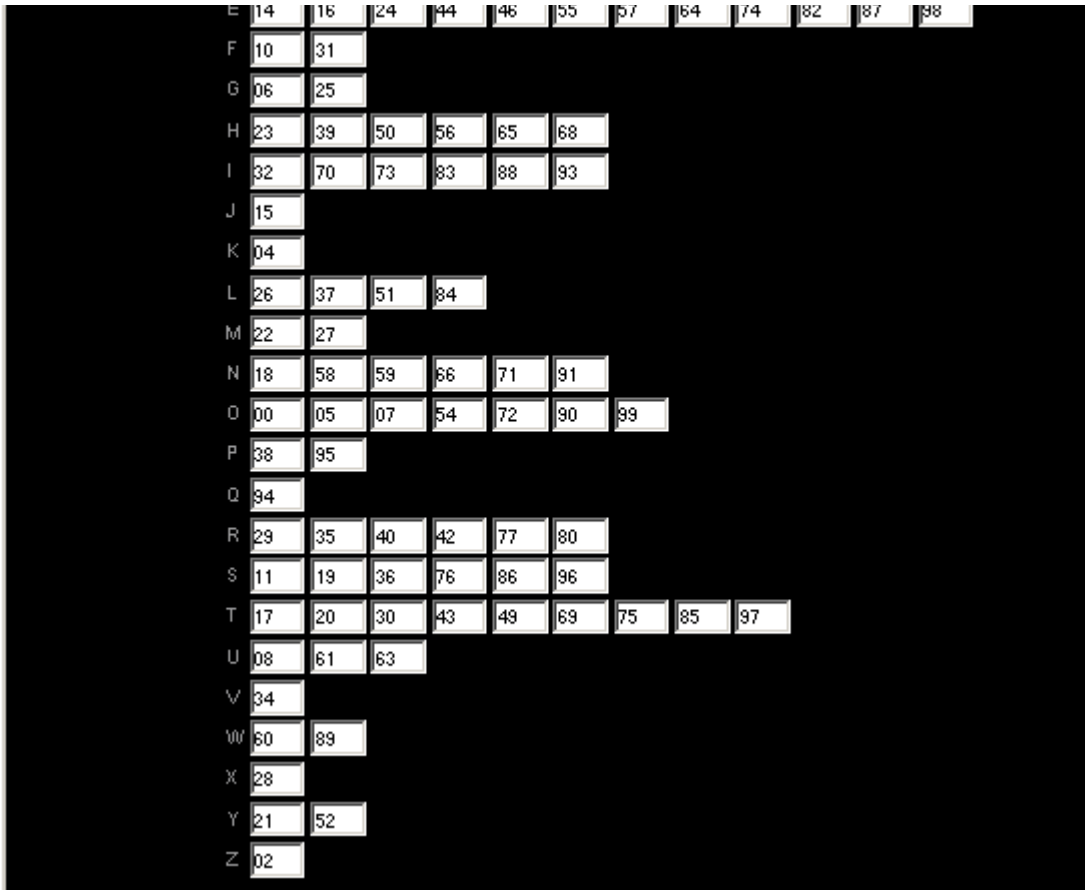
effenen. Het idee is dat als 19% van de letters een *e* is, dat er dan ook 19 symbolen gekozen moeten worden om de *e* te vertegenwoordigen, terwijl er voor de v (2,9%) maar 3 symbolen afwisselend gebruikt hoeven te worden en voor de *q* (0,11%) maar één. Het zou ertoe leiden dat alle letters ongeveer even vaak voor zouden komen in de tekst.
Helemaal veilig is het cijfer daarmee nog niet. Een probleem dat je hiermee niet kunt ondervangen is dat er in de taal bijzonderheden zijn. Zo wordt bijvoorbeeld de letter *q* altijd opgevolgd door de letter*u.* Voor de *q* geldt maar één symbool en voor de *u* maar 2. Door de tekst af te speuren naar een letter die door slechts 2 andere letters gevolgd wordt is de *q* en daarmee de *u* te vinden. Op deze manier konden taalkundigen proberen ook dit cijfer te breken.
Het homofone substitutiecijfer staat ook bekend als monoalfabetisch. De reden hiervoor is dat elk cijfersymbool maar aan één letter kan worden toegewezen ook al zijn er voor bepaalde letters meerdere symbolen beschikbaar. Bij een polyalfabetisch systeem wordt elke letter op meerdere manieren versleuteld, maar elke letter uit het cijferalfabet kan ook aan meerdere klare letters worden toegewezen afhankelijk van de plek in de tekst.

Op de CD-rom is een demonstratie te vinden onder Junior Codebreakers/Homophonic Cipher.

Activiteit

Start de CD-rom onder Junior Codebreakers/Homophonic Cipher en voer een eigen tekst in.
Laat de tekst vercijferen door de tool en beschrijf kort de werking van de tool.
Eventueel kun je ook gebruik maken van onderstaande pagina die wat eenvoudiger van opzet is en geen echte demonstratie laat zien.
Kies voor **Slow Encrypt**





Klik hier om de site te openen.

Over dit lesmateriaal

Colofon

Dit materiaal is achtereenvolgens ontwikkeld en getest in een SURF-project (2008-2011: e-klassen als voertuig voor aansluiting VO-HO) en een IIO-project (2011-2015: e-klassen&PAL-student). In het SURF project zijn in samenwerking met vakdocenten van VO-scholen, universiteiten en hogescholen e-modules ontwikkeld voor Informatica, Wiskunde D en NLT. In het IIO-project (Innovatie Impuls Onderwijs) zijn in zo’n samenwerking modules ontwikkeld voor de vakken Biologie, Natuurkunde en Scheikunde (bovenbouw havo/vwo). Meer dan 40 scholen waren bij deze ontwikkeling betrokken. Organisatie en begeleiding van uitvoering en ontwikkeling is gecoördineerd vanuit Bètapartners/Its Academy, een samenwerkingsverband tussen scholen en vervolgopleidingen. Zie ook www.itsacademy.nl De auteurs hebben bij de ontwikkeling van de module gebruik gemaakt van materiaal van derden en daarvoor toestemming verkregen. Bij het achterhalen en voldoen van de rechten op teksten, illustraties, en andere gegevens is de grootst mogelijke zorgvuldigheid betracht. Mochten er desondanks personen of instanties zijn die rechten menen te kunnen doen gelden op tekstgedeeltes, illustraties, enz. van een module, dan worden zij verzocht zich in verbinding te stellen met de programmamanager van de Its Academy (zie website). Gebruiksvoorwaarden: creative commons cc-by sa 3.0 Handleidingen, toetsen en achtergrondmateriaal zijn voor docenten verkrijgbaar via de bètasteunpunten.

Auteur	Its Academy
Laatst gewijzigd	18 december 2014 om 13:59
Licentie	Dit lesmateriaal is gepubliceerd onder de Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie. Dit houdt in dat je onder de voorwaarde van naamsvermelding en publicatie onder dezelfde licentie vrij bent om: • het werk te delen - te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat • het werk te bewerken - te remixen, te veranderen en afgeleide werken te maken • voor alle doeleinden, inclusief commerciële doeleinden. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveau	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Leerinhoud en doelen	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Eindgebruiker	leerling/student
Moeilijkheidsgraad	gemiddeld
Trefwoorden	e-klassen rearrangeerbaar