01. les 1 de geheime boodschap

Auteur	Its Academy
Laatst gewijzigd	18 december 2014

Inhoudsopgave

Les 1 De Geheime Boodschap

Inhoud van les 1: De geheime boodschap

1.1 Vercijferen of verbergen

Tientallen eeuwen hebben mensen geprobeerd om elkaar boodschappen te sturen die voor anderen verborgen moesten blijven. Daarvoor bedacht men allerlei in wezen verschillende manieren, zoals het verbergen van de boodschap of steganografie en het gebruik van *codes* en *cijfers*.
Een *code* vervangt een boodschap, een enkel woord of een letter door een vooraf afgesproken woord, getal of symbool. Zo wordt de ASCII-tabel gebruikt om een letter of teken te vervangen door een getal en gebruik je een PIN-code als een soort electronische handtekening. Tijdens de Tweede Wereldoorlog stond de code "Operatie Overlord" voor de invasie in Normandië door de geallieerden toen West-Europa nog bezet werd door nazi-Duitsland.
Een boodschap omzetten in iets wat niet meer te begrijpen valt noemen we *vercijferen* of *encryptie*. Het Griekse woord *kryptos* betekent 'verborgen' en de *cryptografie* is de kunst van het schrijven van geheimschrift. De originele boodschap wordt de *klare tekst* genoemd, het systeem om de klare tekst om te zetten heet *de sleutel* en het onleesbare resultaat noemen we de *cijfertekst*. Het terughalen van de klare tekst heet *ontcijferen* of *decryptie*. Het protocol, het geheel van de afspraken die je met elkaar maakt om de originele tekst om te zetten in een cijfertekst, is bepalend voor het *cijfer* of *geheimschrift*.

Meerkeuzevraag

Je bent op visite geweest bij vrienden en gaat laat naar huis. Omdat ze graag willen weten dat je veilig thuisgekomen bent, spreek je met elkaar af dat je de telefoon 2x over zult laten gaan als je thuis bent. Je kunt het 2x bellen opvatten als een:

a. code
a. cijfer
a. verborgen boodschap

Door de eeuwen heen zijn er verschillende methoden bedacht om geheime boodschappen te versturen, maar een van de vroegste vermeldingen van geheimschrift is te vinden bij de Griekse geschiedschrijver Herodotus. In zijn werk *Historiën* beschrijft hij hoe Demaratus, een uit zijn vaderland verdreven Griek die in de Perzische stad Susa woonde, een boodschap stuurde aan de Spartanen in Griekenland om ze te waarschuwen voor een dreigende invasie van de Perzische koning Xerxes I in 480 voor Christus. Omdat het risico van ontdekking groot was schraapte hij de was van een stel tabletten, schreef op het hout wat Xerxes van plan was, bedekte de boodschap opnieuw met was en stuurde de tabletten naar Sparta. Herodotus schrijft dat Corgo, de vrouw van koning Leonidas, na enige tijd raadde dat ze iets zouden vinden als ze de was afkrabden en zo kwam de boodschap aan het licht. De Grieken waren daardoor voorbereid op de aanval van Xerxes. In de slag bij Salamis werd hij door een list afgetroefd al was dat niet direct van doorslaggevende betekenis voor het uiteindelijke verlies van de oorlog een jaar later.

De strategie van Demaratus is een voorbeeld van het verbergen van een boodschap en wordt gerekend tot de *steganografie*, wat letterlijk vertaald 'bedekt schrijven' betekent. Herodotus beschrijft in een ander voorbeeld hoe Histaeus een boodschap stuurde aan Aristagoras van Milete om op te roepen tot een opstand tegen de Perzische koning. Hij liet het haar van een boodschapper afscheren en de boodschap op diens hoofd schrijven. Door te wachten tot het haar weer aangegroeid was kon de boodschapper de boodschap veilig overbrengen. Uiteraard moet je in dit systeem niet al te veel haast

hebben.

In zijn boek *Code* geeft *Simon Singh* mooie voorbeelden van steganografie door de eeuwen heen:

- De oude Chinezen schreven hun boodschappen op dunne zijde, persten het tot een klein bolletje en doopten het in was waarna een boodschapper het bolletje inslikte en overbracht.
- Giovanni Porta beschreef in de zestiende eeuw hoe je een boodschap overbracht door inkt te maken van 30 gram aluin op een halve liter azijn en daarmee op een hardgekookt ei te schrijven. De oplossing dringt door de poreuze schaal en laat een boodschap achter die pas te lezen is als de schaal verwijderd wordt.

Onzichtbare inkt en de microstip, waarin een pagina tekst fotografisch verkleind wordt tot een puntje met een doorsnede van minder dan een millimeter, zijn andere voorbeelden die gerekend worden tot de steganografie. De zwakheid van de steganografie is echter dat, als de boodschap ontdekt wordt, de inhoud ook direct bekend is. Daarom ontwikkelde zich gelijktijdig een manier om de inhoud onleesbaar te maken en dit verstaan we onder cryptografie. De zender en de ontvanger spreken vooraf een protocol af waarmee de boodschap versleuteld en ontsleuteld kan worden. Zonder kennis van het protocol zou het onmogelijk moeten zijn de inhoud van de boodschap te achterhalen.

Meerkeuzevraag

Steganografie is volgens de *Van Dale* een geheime schrijfkunst, maar letterlijk vertaald betekent het*verborgen schrijven*.

Wat valt volgens het bovenstaande onder steganografie?

a. De letters van een woord vervangen door de volgende letter in het alfabet.
a. Een woord vervangen door een ander woord met schijnbaar een heel andere betekenis.
a. Een bericht verstoppen in de dop van een fles en deze versturen.

1.2 Transpositie

Cryptografie kan worden verdeeld in *transpositie* en *substitutie*. Bij transpositie worden letters van de boodschap verwisseld waardoor de tekst onleesbaar wordt. Bij substitutie worden letters vervangen. Een voorbeeld van transpositie is bijvoorbeeld de *hekverplaatsing*, waarin letters van een boodschap om en om op twee regels worden neergezet waardoor iets onleesbaars ontstaat. Hieronder een voorbeeld:

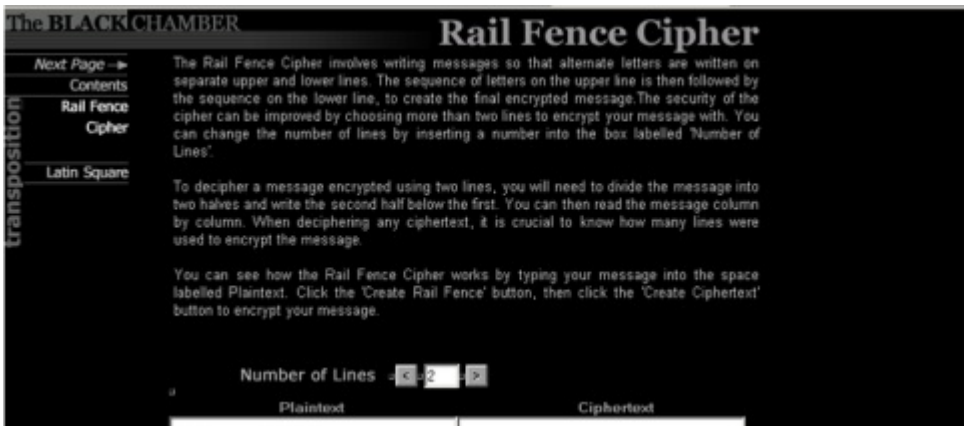
ontmoet me vanavond om zeven uur in cafe de vriendschap

```
o t o t e a a o d m e e u r n a e e r e d c a
 n m e m v n v n o z v n u i c f d v i n s h p
```

ototeaaodmeeurnaeeredcanmemvnvnozvnuicfdvinshp

Het is maar de vraag hoe veilig dit geheimschrift is omdat sommige woorden nog enigszins herkenbaar kunnen blijven. Wellicht dat iemand raden kan dat vinshp weleens zou kunnen staan voor vriendschap. Maar er zijn allerlei variaties te bedenken zoals het drieregelig hek-cijferschrift.

Hieronder een pagina van de site van Simon Singh.
Je kunt een tekst intikken en een aantal regels voor het hek instellen. Het hek wordt zichtbaar in een Pop-up venster.



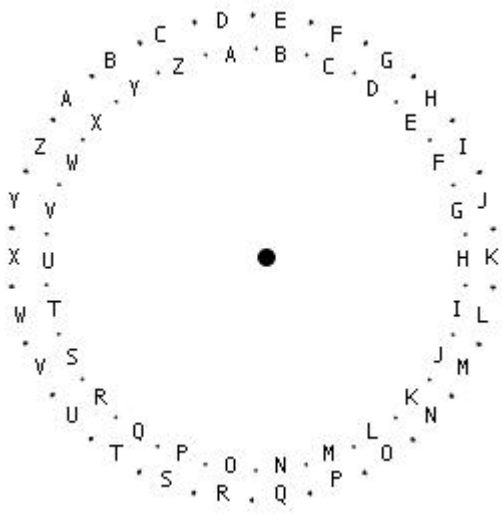
klik hier om naar de site te gaan.

1.3 Substitutie

De tweede tak van cryptografie is de *substitutie* of *vervanging*. Een van de vroegste beschrijvingen komt uit de *Kamasutra*, geschreven in de vierde eeuw na Christus maar gebaseerd op manuscripten uit de vierde eeuw voor Christus. De Kamasutra adviseert vrouwen een aantal kunsten te bestuderen waaronder de kunst van het geheimschrijven. Een aanbevolen methode is het maken van willekeurige letterparen waarbij elke letter wordt vervangen door de gepaarde letter. Zo zou je bijvoorbeeld de letter A kunnen vervangen door een E en de E door de A terwijl je de B vervangt door een W en vice versa. In onderstaande link kun je daar een voorbeeld van vinden.

Het eerste door Suetonius vastgelegde gebruik van het vervangingsschrift voor militaire doeleinden is het Caesar-systeem of het Caesariaanse schuifsysteem, het systeem dat keizer Julius Caesar gebruikte in de Gallische oorlog.

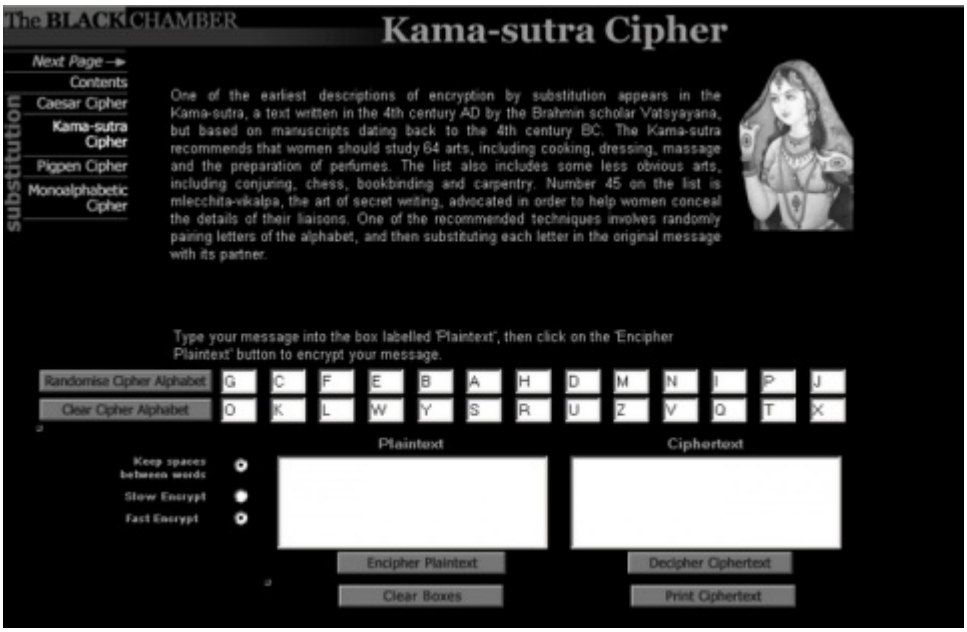
Caesar schoof iedere letter drie plaatsen op in het alfabet. Een A werd dus een D, een B een E, ..., een X werd een A, een Y een B en een Z een C. De beroemde uitspraak "ALEA IACTA EST" (de teerling is geworpen) van Julius Caesar wordt met het Caesar-systeem vercijferd tot "DOHDL DFWDH VWAXQ".



Op de internetpagina hieronder kun je een tekst coderen met het Caesar Cipher. Kies voor *Slow Encrypt* om de werking van het systeem te kunnen volgen. Op de CD-rom(downloaden vanaf de site) staat als extra een demonstratie onder Junior Codebreakers/Caesar Shift Wheel. Daarbij ook een filmpje met een extra toelichting.

Het systeem van Caesar is een speciaal geval van het schuifsysteem. Bij dit cryptosysteem wordt iedere letter een vast aantal plaatsen in het alfabet opgeschoven. Het cryptosysteem is dus: "kies een geheel getal *k* en schuif iedere letter *k* plaatsen op in het alfabet." De sleutel is het getal *k*. Deze is bekend bij zowel de schrijver als de ontvanger, maar moet verder geheim blijven. Bij het ontcijferen schuif je iedere letter weer *k* plaatsen in het alfabet terug.

Wanneer je een boodschap met een schuifsysteem wilt vercijferen, is het handig om twee cirkels met het alfabet met een splitpen op elkaar te maken (*zie de afbeelding hierboven*). Je draait de cirkels zo ten opzichte van elkaar, dat naast iedere letter zijn vercijfering staat, vergelijkbaar met het wiel op de demonstratie.
Klik in onderstaande link het Caesar Cipher aan en oefen nu eerst met het Caesar cijfer.



Klik hier om de link te openen.

Opgave 1

1. Wanneer je een bericht dat vercijferd is met een schuifsysteem wilt ontcijferen, kun je alle 26 sleutels uitproberen. Kun je een snellere manier verzinnen?
2. Probeer de sleutel waarmee onderstaande tekst vercijferd is te vinden. De tekst is vercijferd met een schuifsysteem. Je mag hierbij ook gebruik maken van de tool Caesar Cipher op de bovenstaande Internetpagina.
   JNAAR REWRR RAGRX FGQVR IREPV WSREQ VFZRG RRAFP
   UHVSF LFGRR ZJVYG BAGPV WSRER AVFUR GUNAQ VTRRE
   FGGRX VWXRA ANNEQ RYRGG REFQV RURGZ RRFGR IBBEX
   BZRAM BNYFQ RARAG NYFWR OVWIB BEORR YQJRR GJRYX
   RYRGG REQRR VFXHA WRQRE RFGRR AIBHQ VTURE YRVQR
   A

In het bovenstaande zijn we uitgegaan van een alfabet van 26 letters. Dit is geen noodzaak. Je zou ook kunnen afspreken om bijvoorbeeld leestekens, spaties en cijfers aan je alfabet toe te voegen en zo op een groter aantal 'letters' uitkomen. Uiteraard moet wel bij beide partijen bekend zijn welk alfabet gebruikt wordt.

1.4 Mono-alfabetische substitutie

De kracht van een cryptosysteem hangt af van het aantal sleutels. Het Caesar-systeem heeft maar 25 mogelijke sleutels als je uitgaat van het alfabet van 26 letters. Het aantal sleutels neemt sterk in aantal toe als je iedere verwisseling van letters toestaat. Het cijferalfabet is dan een willekeurige herschikking van het klare alfabet en we noemen dit een mono-alfabetisch substitutiesysteem.

Als je een schikking maakt voor de letters van het alfabet op 26 plaatsen kun je voor de letter *a* 26 plekken bedenken, voor de *b* blijven er 25 plekken over, voor de *c* nog 24 etcetera, tot je voor de *z*uiteindelijk nog 1 plaats overhoudt. Elke mogelijke schikking wordt in de wiskunde een *permutatie*genoemd en het aantal permutaties voor 26 verschillende letters wordt 26! (26 faculteit) genoemd.
Ga na dat 26!=26x25x24x23x.....x3x2x1. In totaal geeft dat meer dan 400.000.000.000.000.000.000.000.000 sleutels. Hier zitten natuurlijk nog wel een heleboel onbruikbare sleutels tussen zoals het klare alfabet zelf, een alfabet waar maar 2 of een paar letters verwisseld zijn, etcetera.


Activiteit

Op de CD-rom staat onder Junior Codebreakers/General Monoalfabetic een toelichting op het monoalfabetisch substitutiesysteem. Je kunt deze ook vinden op de internetpagina van de vorige bladzijde als je klikt op Monoalphabetic Cipher. Het biedt mogelijkheden om hiermee te vercijferen. Onderzoek het codesysteem. Stel de vercijfering eerst in op **Slow encrypt.**

Meerkeuzevraag

Als je de letters van het alfabet uitbreidt met bijvoorbeeld de tekens ! @ # $ % ^ & * (en) dan krijg je een set van 36 symbolen.

Het aantal mogelijke schikkingen wordt daarmee

a. tien keer zo groot
a. 10!=3628800 keer zo groot
a. meer dan 900.000.000.000.000 keer zo groot

Als een substitutiesysteem slechts 25 sleutels heeft dan is het eenvoudig om door proberen het systeem te kraken. Degenen die dat proberen worden wel *cryptoanalisten* of *codebrekers* genoemd, al zou het woord *cijferbreker* beter op zijn plaats zijn. Het domweg uitproberen van alle mogelijke sleutels wordt een *brute force attack* genoemd. In de decryptie van de Caesarcode hierboven heb je in feite op deze manier een aanval uitgevoerd. Je merkt daar al direct het voordeel van de automatisering. Handmatig vraagt een *brute force attack* veel tijd. Het is dan handiger de tekst eerst te analyseren. Een *brute force attack* op een systeem met 26! sleutels waarbij per seconde 1 sleutel zou worden uitgeprobeerd zou 26!/(60x60x24x365) jaar of ruwweg een miljard keer de leeftijd van het heelal vergen.

De eenvoud van het systeem en het vrijwel onbeperkte aantal sleutels maakten het substitutiesysteem in de eerste 1000 jaar na Christus tot een zeer veilig en algemeen gebruikt systeem. Het enige nadeel is dat het lastig is om te onthouden welke sleutel er gekozen is. Een eenvoudiger variant op het systeem werkt met een zogenaamd sleutelwoord of sleutelzin. Door de schikking te laten beginnen met de letters van het sleutelwoord en te laten volgen door de rest van letters van het alfabet, wordt het aantal mogelijke schikkingen veel kleiner maar nog altijd zo groot dat het voor de codebreker onbegonnen werk is de code te kraken. De sleutel is echter makkelijk uit het hoofd te leren en het overbrengen van de sleutel loopt daarom niet het risico ontdekt te worden. Nemen we bijvoorbeeld als sleutelzin: "het is warm voor de tijd van het jaar" dan komt het cijferalfabet er als volgt uit te zien:

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

Afspraak:
In bovenstaand voorbeeld kun je zien dat we ons in deze module houden aan de afspraak om de klare tekst in kleine letters en de cijfertekst in hoofdletters te noteren.

Opgave 2

Verzin met een duopartner een eigen sleutelwoord en maak daarmee een cijferalfabet. De tool helpt je daarbij als je het *Cipher Alphabet* vult en weigert dubbele letters. Spreek met elkaar af dat je elkaar een boodschap stuurt. Voer het gemaakte cijferalfabet in de bovenstaande link bij Monoalphabetic Cipher in en vercijfer je boodschap aan aan je duopartner. Wissel de berichten uit en ontcijfer het bericht van je duopartner.
Werkt het zoals je zou mogen verwachten?

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 13:57
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