

# Opdracht 5: Geheimschrift

Het is niet zo eenvoudig een boodschap aan iemand te versturen als je perse wilt dat iemand anders die niet kan lezen.

Post kan onderschept worden, de telefoon kan afgeluisterd worden en je computer kan gekraakt worden.

Vooraf bij militaire boodschappen die geheim moeten blijven is dat altijd een probleem geweest. Allerlei methoden werden verzonden om berichten geheim te houden. Zo werden heel vroeger slaven kaal geschoren, de boodschap werd op hun hoofd geschreven en als hun haar weer aangegroeid was, werden ze op pad gestuurd om het bericht over te brengen. Onderweg was haren wassen er dan natuurlijk niet bij!

Een methode die steeds weer gebruikt wordt, is het **geheimschrift** of **cryptologie**. In deze opdracht leer je wat meer over de verschillende geheimschriften die in de loop van de tijd gebruikt zijn, welke hulpmiddelen erbij gebruikt werden en hoe je zelf geheimschriften kunt ontwikkelen.

Omdat we in deze opdracht steeds dezelfde uitdrukkingen gebruiken, zetten we ze op een rij met hun betekenis:

*klare tekst* = de boodschap die je wilt versturen, geschreven in gewone taal

*cijfertekst* = de boodschap geschreven in geheimtaal

*ontcijferen* = het omzetten van geheimtaal naar gewone taal

*sleutel* = vaak heb je iets nodig om een boodschap te kunnen ontcijferen, bijvoorbeeld een codewoord. Dit noemen we dan de sleutel.

## Het Caesaralfabet.

Dit is een geheimschrift dat gebruikt werd door Julius Caesar, een Romeins keizer die leefde van 100 tot 44 voor Christus.

Het is een methode die nog steeds gebruikt wordt.

De sleutel is dat elke letter uit de klare tekst vervangen wordt door een letter die 3 plaatsen verder in het alfabet staat.

We geven een voorbeeld van een caesaralfabet.

Je krijgt een briefje in de cijfertekst: VFKLHW HHQV RS!

Om dit briefje te ontcijferen, maken we eerst een schaduwalfabet.

(Onder elke letter komt de letter te staan die 3 plaatsen verder in het alfabet staat, dus bijvoorbeeld de A wordt nu D).

sleutel:	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
+ 3	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

Op het briefje stond dus: SCHIET EENS OP!

### Vraag 1:

Ontcijfer de volgende cijfertekst (geschreven in het caesaralfabet, sleutel + 3):  
RS KHW PDDVODQGFR00HJH NULMJ MH LQ GH EUXJNODV HONH  
ZHHN YLHU OHVVHQ ZLVNXQGH.

Je kunt natuurlijk ook zelf een klare tekst omschrijven naar een cijfertekst. Stel je wilt: BOOM omschrijven, dat wordt dit ERRP (want een B in klare tekst, moet een E worden in cijfertekst).

### Vraag 2:

Zet de onderstaande klare tekst om in cijfertekst (gebruik de sleutel + 3):  
IK ZIT OP DE BASISCHOOL.

Behalve de sleutel + 3, kun je natuurlijk ook andere sleutels gebruiken, bijv. + 10. (Iedere letter wordt dan dus vervangen door de letter die 10 plaatsen verder in het alfabet staat, bijv. A wordt dan K). Soms is dan ook handig om een nieuw schaduwalfabet te maken.

### Vraag 3:

Ontcijfer de volgende cijfertekst (gebruik nu de sleutel +10):  
FSXN TST BOUOXOX YYU JY VOEU?

### Vraag 4:

Zet de onderstaande klare tekst om in cijfertekst (gebruik nu de sleutel + 25):  
VOLGEND JAAR ZIT IK IN DE BRUGKLAS.

Soms kan het ook voorkomen dat je niet weet met welke sleutel een cijfertekst gemaakt is. Je zult dan eerst moeten ontdekken welke sleutel gebruikt is, voordat je de cijfertekst kunt gaan ontcijferen.

In een normale Nederlandse tekst komt meestal één letter het vaakst voor. (Welke letter zou dit nu zijn?).

Als je dus zelf de sleutel moet ontdekken, bekijk je welke letter het vaakst voorkomt, die letter moet dan wel de .... zijn en dan reken je uit welke sleutel het moet zijn.

### **Vraag 5:**

Ontcijfer de volgende cijferteksten (ontdek eerst bij elke zin de sleutel):

- a) LLU LYIPQ ADLL PZ KYPL.
- b) OP NZOP GLY OPKP MZZODNSLA VFY UP KPWQ GTYOPY.

Bij het caesaralfabet werd alleen maar een verschuiving van de letters gebruikt. Je zou natuurlijk ook alle 26 letters van het alfabet door elkaar kunnen gooien. Dan heb je geen 26 mogelijkheden, maar  $26 \times 25 \times 24 \times 23 \times \dots \times 3 \times 2 \times 1$ . En daar komt uit: 403.291.461.126.605.635.584.000.000 (403 kwadriljoen, 291 duizend 461 triljoen, 126 duizend 605 biljoen, 635 duizend 584 miljoen).

Je zou denken dat je zo'n boodschap nooit kunt ontcijferen als je de sleutel niet weet. Maar toch waren er mensen die door tellen hoe vaak een letter voorkomt en veel kennis van de taal toch de oplossing vonden.

Door de jaren heen ontstonden steeds meer "regeltjes".

Zo werd er geen verschil gemaakt tussen hoofdletters en kleine letters en werden de letters in groepjes van 5 bij elkaar gezet.

## De methode van Blaise de Vigenère.

In 1586 bedacht een Fransman, Blaise de Vigenère, een systeem waarbij voor elke letter van de klare tekst steeds een andere verschuiving gebruikt werd.

Bijvoorbeeld 7 plaatsen voor de 1<sup>e</sup> letter, 4 plaatsen voor de 2<sup>e</sup> letter en 10 plaatsen voor de 3<sup>e</sup> letter en dan weer van voren af aan, dus weer 7 plaatsen voor de 4<sup>e</sup> letter. De sleutel is dan: 7 – 4 – 10.

Deze getallen werden dan vaak gegeven in de vorm van een sleutelwoord, in dit geval: *hek*.

De letters van *hek* geven dan de verschuiving aan, de *h* staat 7 plaatsen van de *a*, de *e* staat 4 plaatsen van de *a* en de *k* staat 10 plaatsen van de *a*, de verschuiving is dus: 7 – 4 – 10 vooruit.

Bijvoorbeeld: zet de volgende klare tekst GOEDEMORGEN ALLEMAAL om in een cijfertekst (de sleutel is 1 – 17 – 20 – 6, dus het sleutelwoord is *brug*)

klare tekst:	G	O	E	D	E	M	O	R	G	E	N	A	L	L	E	M	A	A	L
sleutelwoord:	B	R	U	G	B	R	U	G	B	R	U	G	B	R	U	G	B	R	U
sleutel:	1	17	20	6	1	17	20	6	1	17	20	6	1	17	20	6	1	17	20
cijfertekst:	H	F	Y	J	F	D	I	X	H	V	H	G	M	C	Y	S	B	R	F

Als je de cijfertekst ontvangt, zet je het sleutelwoord eerst om in de sleutel.

Vervolgens noteer je het sleutelwoord en de sleutel onder de cijfertekst en ga je de verschuivingen in omgekeerde richting uitvoeren (dus in dit voorbeeld 1 – 17 – 20 – 6 terugschuiven).

### Vraag 6:

Ontcijfer de volgende tekst: (gebruik als sleutelwoord: *geheim*)  
BMLVU MGPUI OQTMZ DMEKR KIZFO K.

### Vraag 7:

Zet de onderstaande klare tekst om in cijfertekst (gebruik als sleutelwoord: *cirkeI*)  
HET MAASLANDCOLLEGE STAAT IN OSS.

## Het cardanrooster.

De wiskundige Hieronymus Cardanus (1501 – 1576) is de vermoedelijke uitvinder van het cardanrooster, een sjabloon dat bestaat uit een vel papier of karton met een aantal gaten. Dit wordt op een leeg vel gelegd en door de gaten wordt de klare tekst geschreven. Na verwijdering van het sjabloon wordt de ruimte tussen deze woorden volgeschreven, zodat het geheel er uit ziet als een onschuldige boodschap. De ontvanger legt eenzelfde sjabloon op de tekst en kan de geheime boodschap door de gaten lezen. De sleutel wordt dus bepaald door het sjabloon.

### Vraag 8: (voor deze vraag moet je eerst blz. 1 en 2 van de bijlage uitprinten!)

Knip de grote rechthoek van de bijlage (blz. 1) uit.

Binnen deze rechthoek vind je kleinere rechthoeken. Knip deze ook uit, zorg wel dat de grote rechthoek heel blijft.

Je hebt nu een sjabloon.

Op de bijlage blz. 2 staat de tekst waarbij je het sjabloon moet gebruiken om de boodschap te lezen.

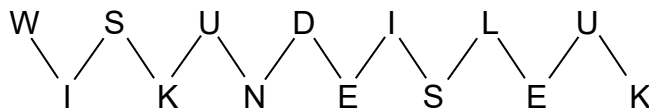
Voer de opdracht die je krijgt ook uit (doe dit pas nadat je alle andere vragen gemaakt hebt). Ben jij op jouw basisschool de enige leerling die meedoet aan dit project, geef dan jouw sjabloon en tekst aan de meester of juffrouw zodat die jouw geheime boodschap kan ontcijferen.

## De hekkode.

Bij de hekkode worden de oneven en even letters van de klare tekst gesplitst door ze in twee regels op te schrijven. De cijfertekst krijg je dan door de bovenste en de onderste regel achter elkaar te zetten.

Bijvoorbeeld: klare tekst: WISKUNDE IS LEUK

wordt:



cijfertekst: WSUDI LUIKN ESEK

Bij het ontcijferen tel je eerst het aantal letters, verdeel je de zin in twee groepen (de bovenste groep is eventueel 1 letter groter dan de onderste groep) en maak je er 1 zin van.

### Vraag 9:

Ontcijfer de volgende cijferteksten.

- GHISH ITEEM CRF.
- DTSEA DRMNE OGHIS HITEE RIEII ENNEE AIRME EMCRF TGBUK N.

## Het rozenkruisersgeheimschrift.

Bij het rozenkruisersgeheimschrift vormt de volgende afbeelding de sleutel:

ABC	DEF	GHI
JKL	MNO	PQR
STU	VWX	YZ

Bij het verscijferen wordt elke letter uit de klare tekst vervangen door het hokje waar de letter in staat met een punt op de plaats die hij in het hokje inneemt, bijvoorbeeld:

A = 

•
---

    B = 

--

    C = 

--

    P = 

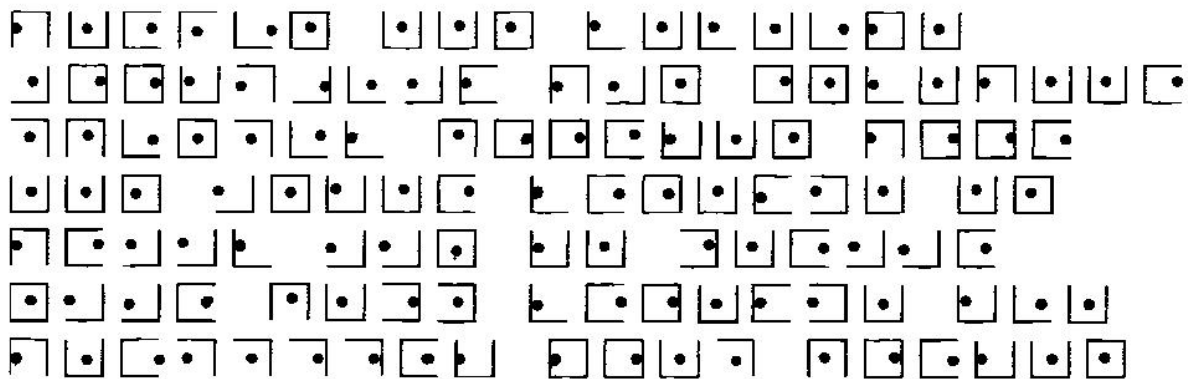
•
---

    W = 

•
---

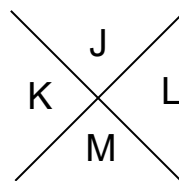
### Vraag 10:

In de onderstaande cijfertekst vind je weer een opdracht. Ontcijfer deze tekst. Voer de opdracht uit (doe dit ook pas nadat je alle andere vragen gemaakt hebt). Ook hier geldt dat als jij de enige leerling bent die dit doet, laat dan weer jouw geheime boodschap ontcijferen door de meester of juffrouw.

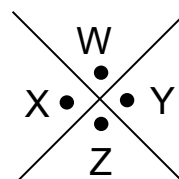


Je kunt op deze manier ook andere sleutels bedenken. Een voorbeeld is:

A	B	C
D	E	F
G	H	I



N	O	P
Q	R	S
T	U	V



## De routetranspositie.

Bij routetranspositie zet men de letters van de klare tekst in een bepaalde volgorde onder elkaar.

(Meestal van links naar rechts, de volgende regel van rechts naar links en dan weer omgekeerd, dus weer van links naar rechts enz.)

De cijfertekst krijg je dan door de letters, gelezen volgens een andere route, weer achter elkaar te zetten. (De route is dan meestal van boven naar onder, de volgende kolom van onder naar boven en dan weer omgekeerd, dus van boven naar onder enz)

In het voorbeeld en de vraag worden steeds 6 kolommen gebruikt.

Bijvoorbeeld: klare tekst: DIT IS GEHEIMSCHRIFT

wordt: D → I → T → I → S → G

↓

S ← M ← I ← E ← H ← E

↓

C → H → R → I → F → T

wordt:

D I → T I → S G

↓ ↑ ↓ ↑ ↓ ↑

S M I E H E

↓ ↑ ↓ ↑ ↓ ↑

C → H R → I F → T

cijfertekst: DSCHM ITIRI EISHF TEG

### Vraag 11:

Ontcijfer de volgende cijfertekst:

(zorg dat je de letters in 6 kolommen zet, tel dus eerst het aantal letters en kijk hoeveel rijen je moet maken).

VGLMS BRUEC IEOIN NUEHG IKERH KTDJE OEITE NTFGM HE

## De kolomtranspositie.

Bij kolomtranspositie gebruik je een sleutelwoord waarin elke letter maar één keer mag voorkomen. Bijvoorbeeld: *wiskunde*.

De klare tekst wordt daar in regels met dezelfde lengte onder elkaar geschreven, eventueel aangevuld met een aantal letters X.

De kolommen worden daarna genummerd volgens de volgorde waarin de letters van het sleutelwoord in het alfabet voorkomen.

De letter die het eerst voor komt, krijgt dan nummer 1, de letter die als tweede voor komt, krijgt nummer 2 enz. In *wiskunde* komt de letter *d* het eerst voor in het alfabet dus de *d* krijgt nummer 1. De letter *e* komt als tweede voor en krijgt dus nummer 2.

Zo krijgt *wiskunde* (alfabetisch wordt dit: *deiknsuw*) dus de code 8 – 3 – 6 – 4 – 7 – 5 – 1 – 2.

De cijfertekst vind je dan door de kolommen van boven naar beneden in volgorde van hun nummer achter elkaar te schrijven. Dus schrijf de letters onder de 1 eerst op daarna de letters onder de 2 enz.

Bijvoorbeeld:

klare tekst: WIE VOOR DE TOEKOMST Kiest, Kiest voor het MAASLANDCOLLEGE

w	i	s	k	u	n	d	e
8	3	6	4	7	5	1	2
W	I	E	V	O	O	R	D
E	T	O	E	K	O	M	S
T	K	I	E	S	T	K	I
E	S	T	V	O	O	R	H
E	T	M	A	A	S	L	A
N	D	C	O	L	L	E	G
E	X	X	X	X	X	X	X

cijfertekst: RMKRLEX DSIHAGX ITKSTDX VEEVAOX OOTOSLX EOITMCX OKSOALX WETEENE

Voor het ontcijferen van de tekst moet je over een sleutelwoord beschikken. Schrijf dan het sleutelwoord op met daaronder de code. Dan moet je de letters van boven naar beneden schrijven. Dan kun je in omgekeerde richting werken tot je de klare tekst hebt.

### Vraag 12:

Ontcijfer de volgende cijferteksten:

- EBX NEX IEI IEH EMX THC SIT DGR (gebruik het sleutelwoord: *wiskunde*)
- IJX HNA IOX SOX BRX EAR JAX TVX (gebruik het sleutelwoord: *brugklas*)

Dit was de laatste vraag over geheimschrift. Als je nog tijd over hebt, kun je nog de opdrachten uitvoeren die je bij vraag 8 en 10 bent tegen gekomen.

Als je dan het geheimschrift nog niet beu bent, kun je zelf nog een andere vorm van geheimschrift maken en vragen voor elkaar bedenken (of voor ons).