CoderDojoBelgium

TOP SECRET !

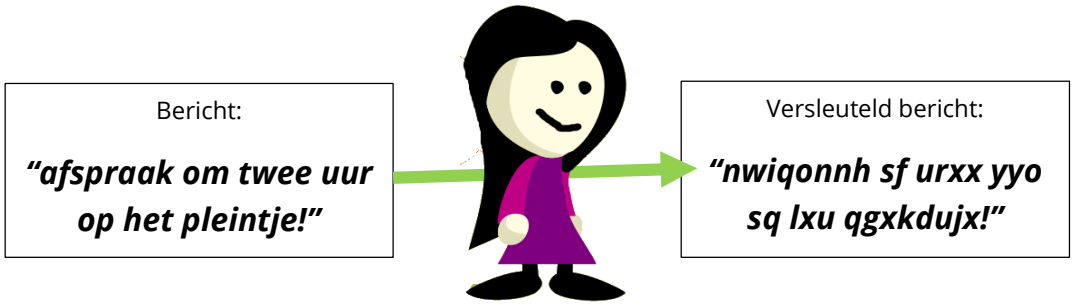
PSSST! GEHEIMPJE!

Je pa die je sms'jes stiekem leest, je juf die liefdesbriefjes onderschept,... Verschrikkelijk vervelend is dat! Gelukkig ben jij ondertussen al een echte programmeur en kan je een programma bouwen om berichten onleesbaar te maken voor alle curieuzeneuzemosterdpotten!

HET PRINCIPE

Anne wil met Brent afspreken, maar ze weet dat meester Charel heel goed is in briefjes onderscheppen... Daarom wil ze het briefje onleesbaar maken voor meester Charel, maar wil ze wel dat Brent kan uitvissen wat ze bedoelt!

Anne zet het bericht eerst om. Dit noemt men **versleutelen**. Ze stuurt een briefje met het versleuteld bericht naar Brent:



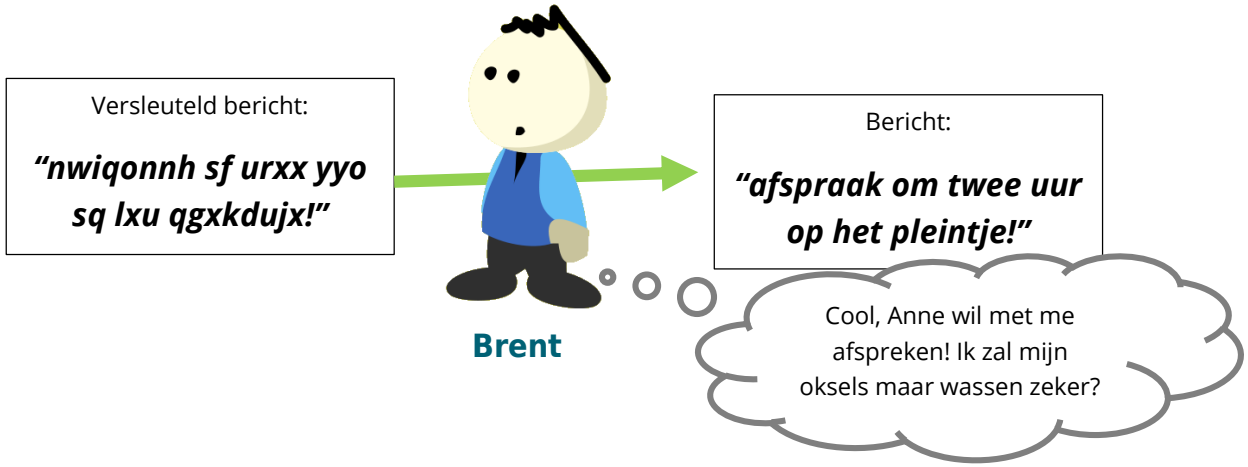
Anne

Moeilijk-woord-van-de-dag-om-mee-te-stoefen-op-familiefeestjes

Versleutelen = vercijferen = encrypteren = encoderen

Een bericht volgens een bepaalde methode omzetten naar een andere vorm. Hierdoor wordt het bericht onleesbaar voor mensen die niet weten hoe ze het moeten ontcijferen.

Als Brent het briefje met het versleuteld bericht ontvangt dan kan hij het met dezelfde methode weer omzetten naar een leesbaar bericht:



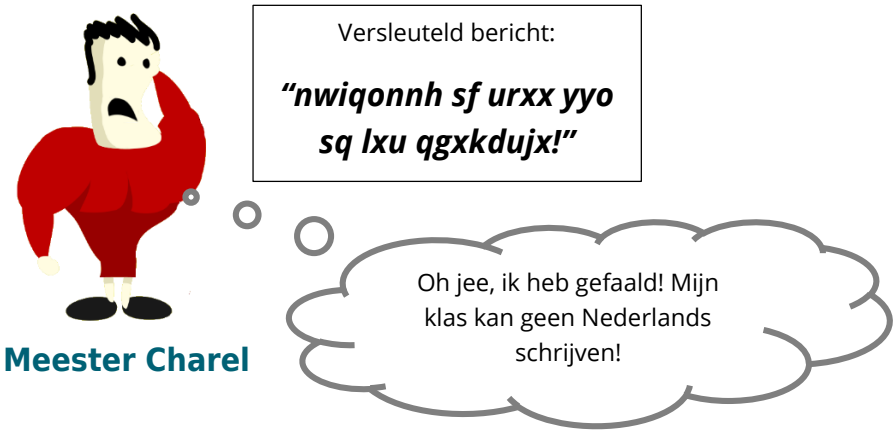
Nog-een-moeilijk-woord-van-de-dag-om-mee-te-stoefen-op-familiefeestjes

Ontsleutelen = ontcijferen = decrypteren = decoderen

Een versleuteld bericht terug omzetten naar een leesbaar bericht.

Het is wel superbelangrijk dat Brent en Anne op voorhand afspreken welke methode ze gebruiken om berichten versleutelen en ontsleutelen. Dit is hun **gedeeld geheim**. Idereen die hun geheim kent kan berichten ontcijferen!

Gelukkig kent meester Charel hun geheime methode niet. Als hij het briefje vindt dan zal hij er wellicht geen jota van snappen:



METHODE OM BERICHTEN TE VERSLEUTELEN

Er bestaan enorm veel manieren om berichten te versleutelen. Wetenschappers zijn constant op zoek naar nieuwe methodes die het nog moeilijker maken voor de 'meester Charels' van deze wereld om onderschepte berichten te ontcijferen.

Anne gebruikte een heel oude **methode** om haar bericht te versleutelen: ze vervangt elke letter van haar bericht door een andere.

Hiervoor heeft ze een **geheime sleutel** verzonnen: een tabel die aangeeft hoe letters vervangen werden:

Letter	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
Wordt	n	b	v	c	x	w	m	l	k	j	h	g	f	d	s	q	p	o	i	u	y	t	r	e	z	a

(geheime tabel om te versleutelen)

Brent kan enkel berichten van Anne ontcijferen als hij haar methode kent (= elke letter vervangen door een andere letter) en als hij haar geheime sleutel kent (de tabel waarin je kan opzoeken hoe letters vervangen werden.

Om berichten te ontcijferen dient Brent dezelfde methode te gebruiken, maar dient hij wel de letters in de andere richting te vervangen:

Letter	n	b	v	c	x	w	m	l	k	j	h	g	f	d	s	q	p	o	i	u	y	t	r	e	z	a
Wordt	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

(geheime tabel om te ontcijferen)

Weetje uit de oude doos

Wist je dat keizer Julius deze methode al gebruikte om geheime boodschappen naar zijn veldheren te sturen? Het feit dat de vijand niet kon lezen maakte deze methode nog extra veilig...

OPGEPAST VOOR VALSSPELERS!

Stel dat meester Charel, in tegenstelling tot de meeste meesters, nogal een slimme kerel is en meteen doorheeft dat Anne gewoon letters vervangen heeft. Kan hij het bericht ontcijferen zonder dat hij de geheime tabel kent?

Da's een heel goeie vraag! Hoeveel mogelijkheden zijn er eigenlijk om letters te vervangen? Om de 'a' te vervangen kan je nog kiezen uit alle letters, dat zijn er in ons alfabet 26. Als je een vervangletter voor 'a' hebt gekozen blijven er nog 25 letters over waarmee je de 'b' kan vervangen. Voor de 'c' blijven er nog 24 over en zo verder.

Het aantal manieren waarop je een vervangtabel kan opstellen is: **26 x 25 x 24 x 23 x 22 x 21 x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1**. Probeer dat maar eens uit te rekenen op je rekenmachine: het resultaat is **403291461126605635584000000**, en dat is redelijk veel!

Wiskundeweetje

26 x 25 x 24 x ... x 1 noemt men **de faculteit van 26** en kan je ook schrijven als "**26!**"

Als meester Charel supersnel zou werken (ook iets wat de meeste meesters niet doen) en elke minuut een nieuwe sleutel zou proberen dan zou hij meer dan 750 miljard keer een miljard jaar bezig zijn om alles te proberen! Zoveel geduld heeft hij waarschijnlijk niet... Zelfs voor een supersnelle computer is het in de praktijk onmogelijk om alle combinaties te proberen.

Meester Charel zou wel ongelooflijk veel geluk kunnen hebben, en meteen al per toeval de juiste combinatie kiezen! Maar die kans is heel heel klein...

Er is wel een slimmere manier om deze methode te **kraken**: sommige letters komen meer voor in het Nederlands dan andere. Zo wordt de letter 'e' het vaakst gebruikt (gemiddeld zijn 18,91% van alle letters in een Nederlandse tekst een 'e') en de letter 'q' het minst (zo'n 0,009%).

Als je genoeg geheime berichten onderschept kan je dus de betekenis van een geheim teken achterhalen door te tellen hoe vaak dit teken voorkomt. Daarom wordt het vervangen van letters niet meer als een veilige methode beschouwd om superbelangrijke berichten te versleutelen. Voor liefdesbriefjes is het echter nog steeds een aanrader ☺

ZELF AAN DE SLAG IN SCRATCH

Jij hebt alles in huis om een vercijferaar in Scratch te maken! Wil je dat doen zonder hulp? Cool, begin er maar aan!

Toch wat hulp nodig? Volg dan deze stappen. Niet alles wordt tot in de puntjes uitgelegd, hier en daar mag je zelf nog een beetje nadenken ;-)

FIRST THINGS FIRST

Beginnen met het belangrijste. Geheime berichten versturen en ontcijferen is echt iets voor geheime agenten. Geef je kat een ultra-coole geheim-agent-look! Blote katten zien er niet zo stoer uit...

BERICHT INGEVEN

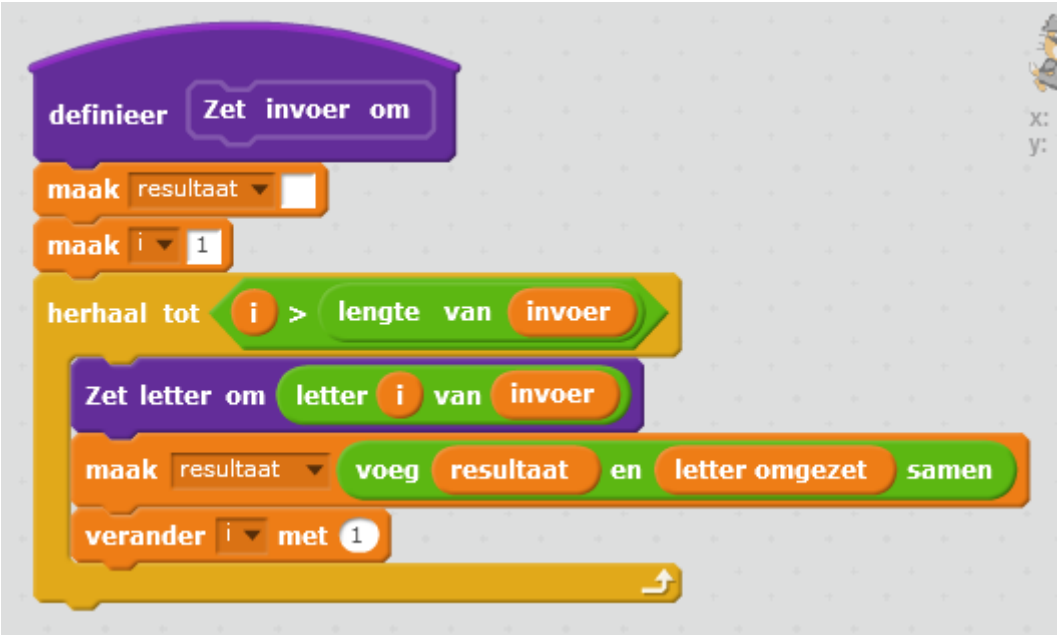
Laat je kat vragen om een bericht in te geven en bewaar het antwoord in een variabele 'invoer'.

BERICHT OMZETTEN

Maak een variabele ‘resultaat’. Deze zal later het omgezette bericht bevatten. Maak alvast een blokje ‘Zet invoer om’ en maak het resultaat gelijk aan de invoer. Zorg ervoor dat je kat het resultaat zegt:

Nog niet zo spannend... De kat zegt gewoon terug wat je hebt ingegeven. Zo’n geheim bericht zal meester Charel nog makklijk kunnen ontcijferen.

We dienen het ‘Zet invoer blokje’ aan te passen zodat het elke letter van de invoer omzet naar een geheime letter:



Om letter per letter over de invoer te lopen gebruiken we een tijdelijke variabele ‘i’. Die zetten we eerst op 1 en zolang i kleiner is dan de lengte van de invoer kunnen we met het blokje ‘letter _ van _’ een bepaalde letter van de invoer opvragen.

Het blokje ‘Zet letter om’ maakt van een letter van de invoer een andere letter en bewaart deze in de variabele ‘letter omgezet’. Elke omgezette letter wordt achter het resultaat geplakt met het blokje ‘voeg _ en _ samen’.

‘Zet letter om’ is een blokje dat we nog zelf moeten maken. Een eenvoudig voorbeeldje vind je hiernaast. Hierbij wordt een ‘a’ omgezet in een ‘e’ en een ‘e’ in een ‘a’. Alle andere letters bijven onveranderd.

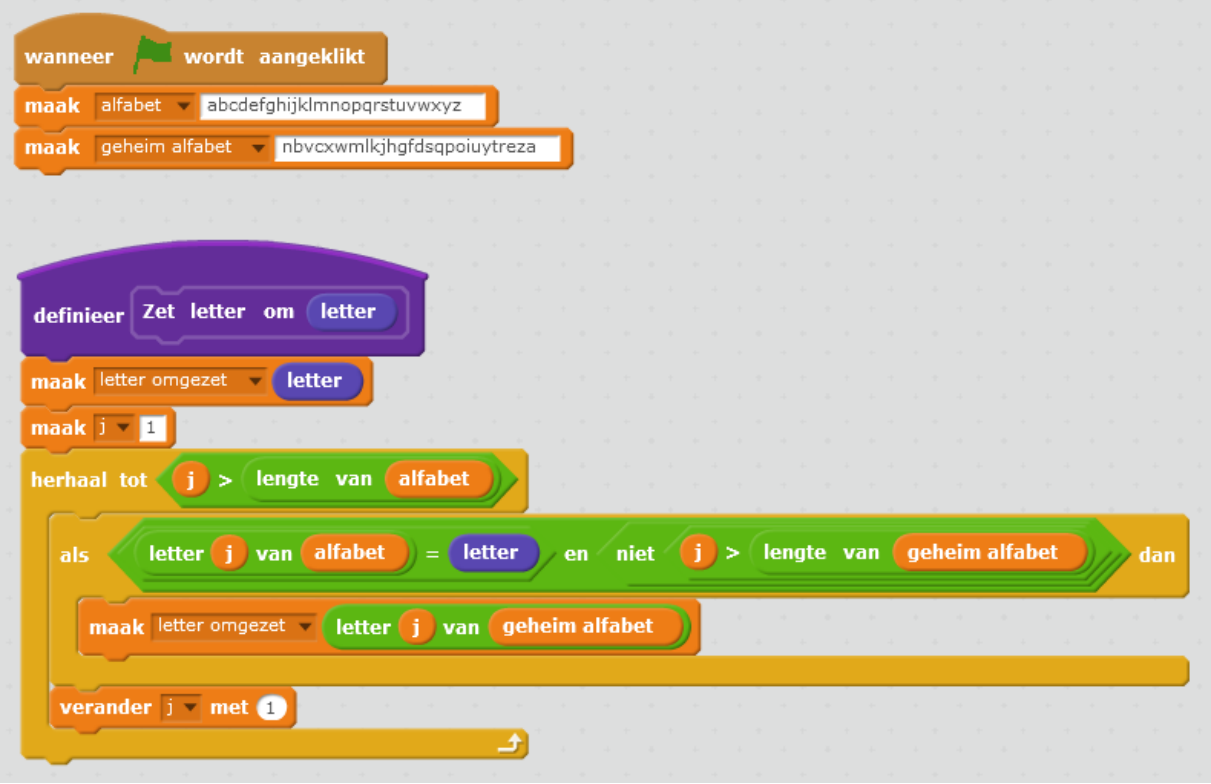
Scratch-tip - Scratch maakt geen verschil tussen hoofdletters en kleine letters het blokje ‘letter = a’ zal dus ook waar zijn als ‘letter’ een hoofdletter ‘A’ is. Dat is niet zo in alle programmeertalen. Zo is JavaScript bijvoorbeeld wel **hoofdlettergevoelig**: voor JavaScript is een ‘a’ niet gelijk aan een ‘A’. Meesters en juffen zijn meestal ook hoofdlettergevoelig…

Je kan al testen!

UITBREIDEN

Je kan het 'Zet letter om'-blokje uitbreiden om meer letters om te zetten. Hoe meer letters je omzet, hoe moeilijker het is om je geheime bericht te kraken!

Als je wil kan je dit doen door meer 'als-dan'-blokjes te gebruiken, maar je kan het ook slimmer aanpakken. Begrijp je wat deze blokjes doen?



Je zou het op nog een andere manier kunnen maken door lijsten te gebruiken.

UMDREHEN

Als je een geheim bericht ontvangt, moet je het natuurlijk ook terug kunnen ontcijferen! Je mag helemaal zelf verzinnen hoe dat moet. Beetje hulp nodig? Op **scratch.mit.edu/projects/88418014** kan je spieken ☺