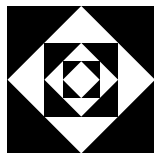
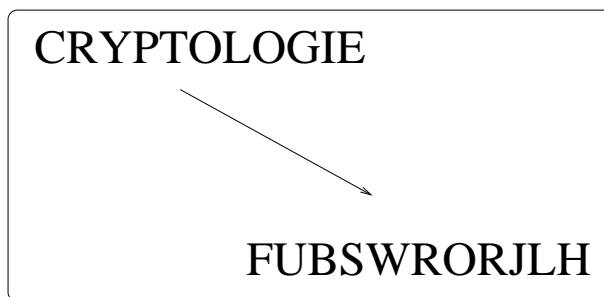


Cryptologie

Maurice Alberts
Joost Langeveld



Stichting Vierkant voor Wiskunde

Voorwoord

In dit onderzoeksprogramma ga je aan het werk met één van de basisbeginselen van de cryptologie, de mono-alfabetische substitutie.

De mono-alfabetische substitutie is, het woord zegt het al, een substitutiemethode. Dit wil zeggen dat letters vervangen worden (meestal door andere letters). Hoe je dit doet, dat kun je verderop lezen.

Als je meer opgevas wilt doen: achterin staan nog wat extra opgaves. En je kunt natuurlijk ook altijd zelf opgaven maken om die dan aan anderen te geven.

Nog iets over het woordgebruik:

Klare tekst: hiermee bedoelen we de gewone Nederlandse tekst die niet gecijferd is. Met **gecijferde tekst** bedoelen we het resultaat van het gecijferen van een klare tekst: de onleesbaar gemaakte tekst. Bij **substituties** worden letters vervangen door andere symbolen.

Vind je dit een leuk onderzoeksprogramma, dan kun je ook eens het doeboekje cryptologie proberen. Dit is te bestellen bij Vierkant.

Veel plezier ermee!

Maurice en Joost.

Hoofdstuk 1

Mono-alfabetische substitutie

1.1 Inleiding

In het vorige hoofdstuk zagen we methoden waarbij alleen de volgorde van de letters werd veranderd. De letters zelf werden niet veranderd. Een andere manier om teksten te verscijferen is de letters vervangen door andere tekens. Zo maak je eigenlijk een nieuw ‘alfabet’.

Voorbeeld.

We vervangen letters door getallen op de volgende manier:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

En we zien:

D I T I S W E L E R G S I M P E L
04 09 10 09 19 23 05 12 05 18 07 19 09 13 16 05 12

Met getallen is het makkelijker om codes te maken. Bijvoorbeeld door optellen (zie Caesar-code). We zullen deze manier van het omzetten van letters in getallen verderop vaker gebruiken.

In plaats van het vervangen van letters door getallen of andere vreemde tekens, kunnen we de letters ook vervangen door andere letters. Je ziet dan alleen letters, maar kunt de boodschap toch niet direct lezen. We noemen dit *mono-alfabetische substitutie*.

1.2 Verschuiving

Een voorbeeld van zo'n substitutie is de *Caesar-code*. Volgens de geschiedenisboekjes gebruikte Julius Caesar rond 50 voor Christus de volgende code:



A	B	C	D	E	...	V	W	X	Y	Z
↓+3	↓+3	↓+3	↓+3	↓+3		↓+3	↓+3	↓+3	↓+3	↓+3
D	E	F	G	H	...	Y	Z	A	B	C

Iedere letter wordt drie plaatsen verder geschoven in het alfabet. Als je voorbij de 'Z' gaat, begin je weer opnieuw bij de 'A' te tellen. Deze code heet dan ook wel de *Caesar-3* of kortweg C^3 code, omdat je de klare tekst over drie plaatsen verschuift.

Voorbeeld.

HET IS NU AUGUSTUS

wordt

KHW LV QX DXJXVWXV

Je ziet 'H' + 3 = 8 + 3 = 11 = 'K'.

Als je tekst wilt ontcijferen, dan moet je in plaats van drie bij iedere letter optellen, drie van iedere letter aftrekken.

Voorbeeld.

FRPSXWHU

wordt

COMPUTER

Je ziet 'F' - 3 = 6 - 3 = 3 = 'C' enzovoorts.

Opgave 1

Ontcijfer met de C^3 -code:

G H C H R S J D Y H L V Q X R S J H O R V W, R S

Q D D U G H Y R O J H Q G H!

★ Opgave 2

Hoeveel verschillende codes kunnen er op deze manier gemaakt worden?



Deze code kan nog iets verbeterd worden (moeilijker te kraken gemaakt) door niet alleen de letters te vercijferen, maar ook de spatie te laten 'meedraaien'. Geef de spatie dan nummer 27 en verder gaat alles zoals hierboven. Je kunt dan veel moeilijker zien waar het ene woord eindigt en het volgende begint. Een andere verbetering is om de spaties tussen de woorden gewoon weg te laten.

Soms weet je alleen dat een bepaalde tekst met een Caesar-code is vercijferd, maar niet met welke Caesar-code. Je kunt dan toch de klare tekst terug vinden. Dit doe je als volgt:

- Schrijf het eerste woord (of bijvoorbeeld de eerste tien letters) bovenaan een leeg blaadje.
- Schrijf nu hieronder dezelfde tekst, maar dan alle letters 'één letter verder'. 'A' wordt dan 'B', 'B' wordt 'C' enzovoorts.
- Herhaal dit totdat je een regel krijgt met normale Nederlandse woorden. Dit is dan de juiste verschuiving. Nu kun je de rest van de tekst ontcijferen.

Voorbeeld.

De versleutelde tekst FGVVEDFFZVCVEKVURX is vercijferd met een Caesar-code. Met de methode van hierboven wordt dit:

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

En je ziet dat de klare tekst OP EEN MOOIE LENTEDAG was.

Opgave 3

Gebruik de hierboven genoemde methode om de volgende Caesar-code te kraken. Welke Caesar-code is er gebruikt?

```
G Z Z N W V V M
```



Opgave 4

Bedenk zelf een zin en vercijfer deze met een Caesar-code. Je mag zelf kiezen welke Caesar-verschuiving je gebruikt en of je de spatie laat meedraaien.

1.3 Andere substituties

Omdat er maar een klein aantal verschillende Caesar-codes zijn, is deze simpel te kraken. Gelukkig zijn er ook andere manieren om de letters van het alfabet te verwisselen, bijvoorbeeld een spiegeling ('A' wordt 'Z', 'B' wordt 'Y', 'C' wordt 'X' tot en met 'Z' wordt 'A'). Deze code heet ook wel de *Atbash-code*.

Opgave 5

Wat betekent de volgende tekst in Atbash-code?

W R G R H V V M Z G Y Z H S E V I X R Q U V I R M T.

Maar ook deze code is niet echt moeilijk, omdat de letters nog steeds in de juiste volgorde staan. Dit hoeven we natuurlijk niet zo te doen. De code wordt al een stuk beter als we een substitutie hebben waar geen regelmaat in zit. Om zo'n substitutie te onthouden, kun je een tabel maken zoals in het begin van dit hoofdstuk. Als iemand echter die tabel vindt, is je code gekraakt en dat willen we natuurlijk niet! Je wilt eigenlijk de substitutie makkelijk kunnen onthouden zodat je hem niet op hoeft te schrijven. Dat kan weer met een sleutelwoord.

Voorbeeld.

De sleutelzin is DIT IS TE MOOI OM WAAR TE ZYN . Dit geeft in een tabel

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

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

We schrijven de letters van de sleutel achter elkaar. Als we een letter al gehad hebben, dan slaan we die over. Als de sleutel-tekst op is, zetten we alle letters die we nog niet gebruikt hebben erachter. Dan zet je het alfabet in gewone volgorde eronder, en je hebt een code. Hierbij staat er 'Y' geschreven in plaats van 'IJ'. Dit is om het kraken van de code te bemoeilijken.

Een tekst versleutelen doe je door een letter van de klare tekst in de onderste rij op te zoeken. De letter die er boven staat schrijf je dan op.



BYNA wordt IVBD.

Ontcijferen doe je door in het bovenste ‘alfabet’ de code-letter op te zoeken en dan te kijken welke letter daar onder staat.

ZYDDH wordt KLAAR.

Korter gezegd: ontcijferen doe je van boven naar beneden, vertcijferen doe je van beneden naar boven.

Opgave 6

Codeer de volgende tekst met de ‘DIT IS TE MOOI OM WAAR TE ZYN’-sleutel:

DIT IS TE MOOI OM WAAR TE ZYN.

Opgave 7

Decodeer de volgende tekst met de ‘DIT IS TE MOOI OM WAAR TE ZYN’-sleutel:

EEB PCCHIEEYS PDB EEB TCSEQCCHS JLIJKAKLKAЕ.

Opgave 8

Waarom moet je geen korte sleutel kiezen of een sleutel waarbij je bijvoorbeeld alleen de eerste tien letters van het alfabet in je sleutel gebruikt?

Opgave 9

Hoeveel verschillende codes kun je maken, als je willekeurige mono-alfabetische substituties gebruikt?



1.4 Codes kraken: frequentie-analyse

Stel nu eens dat je weet dat een tekst versleuteld is met een mono-alfabetische substitutie, maar je weet de sleutel niet. Hoe kun je nu de tekst ontcijferen? Als we helemaal geen extra informatie hebben zou dit erg moeilijk zijn. Gelukkig hebben we een paar hulpmiddelen:

- De teksten die we willen ontcijferen zijn vaak geen willekeurige rijen van letters. Het zijn (Nederlandse) woorden en zinnen. Zeker als de verschillende woorden door spaties worden gescheiden, kom je een heel eind als je eenmaal een paar letters weet.
- Een ander hulpmiddel kan bijvoorbeeld zijn dat je weet dat de gecodeerde tekst een brief is. Bovenaan een brief staat vaak een plaats vanwaar hij verzonden is. Als je die plaats weet, kun je al een aantal letters plaatsen in de substitutietabel.
- Een heel belangrijk hulpmiddel bij het kraken van dit soort codes is het feit dat niet iedere letter even vaak voorkomt in een normale tekst. Je ziet dat er op deze bladzijde erg veel letters 'E' staan, terwijl er bijna geen 'X' op staat. In het Nederlands komen de letters 'E', 'N' en 'A' het meest voor. Voor elke taal zijn de frequenties waarmee letters voorkomen in een tekst verschillend. Er worden tabellen van deze frequenties gemaakt door in verschillende soorten teksten het aantal letters te tellen. Bijvoorbeeld rapporten van ministeries, kranten en schoolboeken.

De volgende tabel geeft aan hoe vaak een bepaalde letter gemiddeld voorkomt in een Nederlandse tekst van 10000 letters lengte:

A	B	C	D	E	F	G	H	I	J	K	L	M
794	135	102	580	1940	59	296	367	611	213	251	370	238
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1000	580	139	0	597	335	604	157	192	191	1	1	241

Hoe kun je dit nu gebruiken om een tekst te ontcijferen? Eerst tel je in de gecodeerde tekst hoe vaak iedere letter voorkomt. Letters die vaak voorkomen in de gecodeerde tekst, hebben een grote kans om een letter voor te stellen die vaak voorkomt in het Nederlands. De letter die het meest voorkomt in een tekst is ook meestal de code voor de letter 'E'. Vanaf hier is het vooral veel proberen. Vaak kun je een paar woorden herkennen zoals 'een', 'van' of 'de'. Hiermee kun je de substitutie verder uitwerken, weer nieuwe letters vinden, daarmee weer woorden herkennen enzovoorts. Soms kun je zelfs een goede gok maken naar wat de sleutel was.

Schrijf de gecodeerde tekst nog een keer op, maar schrijf in plaats van de letters van de gecodeerde tekst nu alleen puntjes. Hierop kun je dan straks de letters invullen die je gevonden hebt. Nadat je bedacht hebt welke letter waarschijnlijk de 'E' is ga je verder en gok je steeds welke letter een codeletter voorstelt en vult dit in op de puntjes. Gebruik een potlood, dan kun je het nog uitgummen als je verkeerd gegokt hebt. Deze manier van code-kraken heet ook wel *frequentie-analyse*. Het werkt beter naarmate de tekst langer is.

**Opgave 10**

Bij deze opgave moet je een tekst die met een mono-alfabetische substitutie gecodeerd is ontcijferen. Dit is wel aardig wat werk! De versleutelde tekst is:

A F J B A X X O Y G E H X X O X X J N F Q I F Y O R G B
S X J T X Z N Q T K K O A F J G J Z K H L R Q F O P F J
S X J L G J Z K A F P Y G E N F Q K L J F H F J S X J
I F C A .

Hoofdstuk 2

Extra opgaven

Opgave 11 Vercijfer de volgende tekst met ‘Caesar 7’.

D I T I S E E N C A E S A R S U B S T I T U T I E

Opgave 12

Decodeer de volgende tekst. Hij is vercijferd met ‘Caesar 23’

D O L B Q B K R F Q W X K A S L L O Q

Opgave 13

Decodeer de volgende tekst. Hij is vercijferd met een onbekende Caesar.

B W S H C T B C C W H U S K S S G H

Opgave 14

Het volgende spreekwoord staat in ‘Caesar 9’. Maak het af (vercijferd natuurlijk).

Q X P N K X V N W . . .

Opgave 15

Decodeer de volgende Caesar substitutie.

N A W J C S F L N G G J O A K C M F V W

**Opgave 16**

Decodeer de volgende tekst. Het is een Atbash substitutie.

G D V V G B R H V V M O L L M V B G F M V

Opgave 17

Ook bij deze opgave is de Atbash-code gebruikt.

D R V D R O V I V V M K L G Q V Y I R W T V M?

Opgave 18

Ontcijfer de volgende tekst. Het is een monoalfabetische substitutie.

G F X R U R R K P V R R E Q O Z R F E B A A K X R C R E R F
V A M N R R C X A C C O R (Z G N R R P P R I K A F L K O B L
P G R F) S R Z R P E G G K M G C E A P R F U A F T A R M A K,
E R K G D R O F M R U R C E N R R K. N R R C X A C C O R?
F R R, R R F L C R O F R F R E R K Z R P P O F X S C R R I
D G R E O X V R R K M P A F E S O R E R F A A F E R
G U R K V R C E O X R K M R F D A A L P R N R P C R U R F
U A F E R K G D R O F R F O F E R G D K O F X R F E R
C R X R K H C A A P M R F S R H A A C E F O R P
X R D A L L R C O B L.

Opgave 19

Bij deze Caesar draait de spatie ook mee!

N Y V L L U G B H U G Q V V Z G L U G T H A Y P J L

**Opgave 20**

Dit is een monoalfabetische substitutie. Kun je hem aan?

B F O I L L H A H X G H B F O Y U P H A H X B F O H U G H X

B F O Y Y U D H U B F O P H U P Q T. B F O C L H A U C F O H X G

B F O Y Y L B F O U H W P H U P M H B F O Y Y U W H H B L H A

L Y H. B F O Y Y A J Y H L H X G B F O I P J H X G

B F O Y Y U U Y T C C U P X.