

Cryptografie

door Henri Dehenauw

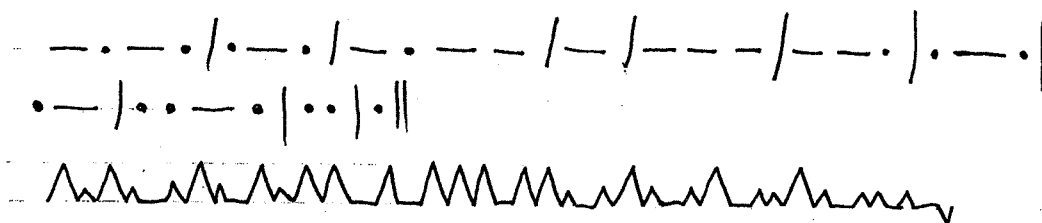
uit het Grieks, de samenstelling van woorden kryptos (= verborgen) en grafein (= schrijven) betekent verborgen schrijven of m.a.w. geheimschrift.

Dat er ontelbare mogelijkheden zijn, hoeft geen betoog, van het eenvoudig geheimschrift -zoals wij die gebruiken - tot het zeer ingewikkeld geheimschrift, gebruikt door spionnen.

Laat ons enkele mogelijkheden overlopen.

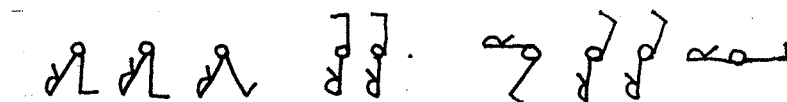
1. Morse, waar men verschillende mogelijkheden heeft om het grafisch voor te stellen, is best bruikbaar bij een spel.

vb.



2. Ook het Semafoor seinstelsel is bruikbaar als geheimschrift. Men stelt de armstanden schematisch voor. Let wel op dat er een goed onderscheid is tussen linker- en rechterarm.

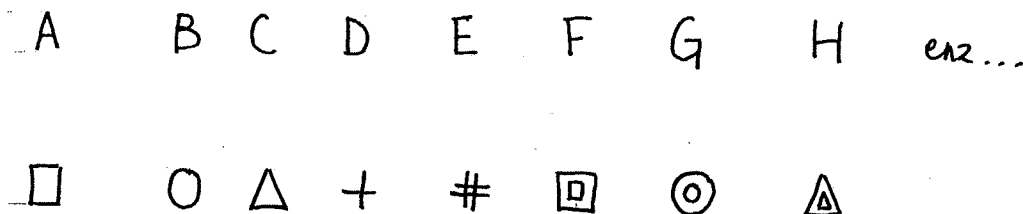
vb.



Deze methoden zijn echter niet te klasseren onder geheimschrift, daar beide bij velen bekend zijn, o.a. bij diegenen, die in bij een jeugdvereniging geweest zijn.

3. Meer zekerheid van geheimhouding heeft men, wanneer - bv. binnen de eenheid-afgesproken is dat aan elke letter van het alfabet een bepaald teken (symbool) toebedacht is. Het nadeel van deze methode is wel, dat wanneer men de afgesproken sleutelcode vergeet of verliest men niet in staat is het bericht te oncijferen.

vb.



4. Het alfabet zelf biedt tal van mogelijkheden.

vb1.

Men schrijft het alfabet in volgorde, vervolgens schrijft men onder elke letter een nummer. In het bericht schrijft men dan i.pl.v. letters, cijfers

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	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

wat betekent: 19-5-1 19-3-15-21-20-19

vb2.

men kan de cijfers vervangen door het alfabet in omgekeerde orde, zodoende krijgt men:

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

wat betekent: DZMWVOZZI ZMPVIH OLH

vb3.

Men kan een geschreven bericht gewoon in spiegelschrift schrijven - moet je echt eens proberen - of gewoon ieder woord omgekeerd schrijven

wat betekent: EID TID NAK NEZEL, SI PANK

vb4.

Soms maakt men gebruik van een geschreven tekst (bv. krantenknipsel). Men schrapt, doorpikt of duidt aan, in de leesrichting, welke letters men nodig heeft.

EEN GOEDE SCOUTS WEET MET ALLER RAAD, HET WOORD ONMOGELIJK BESTAAT VOOR HEM NIET....

betekent: ga waar...

vb5.

Men kan met getallen de nodige letters uit een tekst aangeven, waarbij men telkens na het vinden van een letter, opnieuw start met tellen tot de volgende letter. (zie tekst vb4.)

dat geeft dan : 4 - 17 12-16-17-4

5. Een ander soort geheimschrift is het onzichtbaar bericht, geschreven met melk of citroensap. Om het bericht te kunnen lezen moet men het papier, waar de boodschap op geschreven staat, boven een kaars of aansteker verwarmen (pas op dat ge het papier niet in brand steekt!)

6.Sleutel- of codewoorden

Men kan gebruik maken van sleutel of codewoorden om een geheimschrift op te stellen. Met deze methode geeft men een nummer aan elke letter van het sleutelwoord of -zin. Zorg wel dat eenzelfde letter geen tweemaal genummerd wordt. Een briefhoofd kan bijvoorbeeld zeer goed dienen; eventueel ontbrekende letters worden in het bericht tussen de nummers geschreven.

vb.

~~DE BAGGERFIRMA CLOETENS NV~~
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

~~ANTWERPSE KAAI~~
17 18 19

~~ZEEBRUGGE~~
20 21

ontcijfer: 5-4 14-4-4-6 H-2-13 11-12-19-4-4-11

7. Roosters

Voor een geheimschrift wordt regelmatig gebruik gemaakt van een rooster met x- en y-as. Het eerste sleutelwoord schrijft men steeds op de x-as; het tweede op de y-as. Men kiest woorden waar in éénzelfde woord een letter maar éénmaal voorkomt.

vb1. met sleutel: ZEFIR & KLAVER

	Z	E	F	I	R
K	a	b	c	d	e
L	f	g	h	i	j
A	k	l	m	n	o
V	p	q	r	s	t
E	u	v	w	x	y
R	z				

de lettergroepen LE-KZ AI-KZ-KZ-VF LF-EZ-LI-VI

betekent: ga naar huis

neem nu LE: uit de "L" van klavier trekt men een denkbeeldige lijn naar rechts en uit de "E" van zefir trekt men een denkbeeldige lijn naar beneden, in het kruispunt vindt men de letter "g". Doe nu het zelfde met de andere lettercombinaties

vb2. een variant op de roostercodering is door het alfabet in groepen van bv. 5 letters te verdelen over het rooster (men zou het code 5 kunnen noemen)

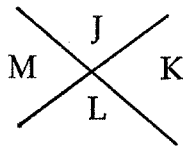
	1	2	3	4	5
A of 1	a	b	c	d	e
B of 2	f	g	h	i	j
C of 3	k	l	m	n	o
D of 4	p	q	r	s	t
E of 5	u	v	w	x	y
F of 6	z				

gebruikt men nu op de x-as de nummers en op de y-as de letter dan vertaalt men :
"Aan de heer" tot : A1-A1-C4 A4-A5 B3-A5-A5-D3

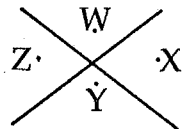
of in het geval van cijfers op de y-as: wordt dit: 1.1-1.1-3.4 1.4-1.5 2.3-1.5-1.5-4.3




vb3. Bij een ander voorbeeld gebruikt men een andere vorm van rooster

A	B	C
D	E	F
G	H	I



N.	O	P
Q.	R	S
T.	U	V



A wordt geschreven als , B als  en N als  (merk het puntje op)

ontcijfer: 

Zo als je alles aandachtig gelezen hebt, denk je dan dat je onderstaande cryptogrammen kunt ontcijferen? Bedenk dat het er vooral op neer komt dat men eerst eens goed nadenkt en probeert na te gaan wat men in handen heeft: onleesbare woorden kunnen misschien achterste voren gelezen worden, enkelvoudige cijfers betekenen alfabet genummerd, enz...

A₁₄ - 12 - 8
B₁₄ - 12 - H
K₃D - 2C - M₅
2C₁₆ - 7 - MN₄₄ - 7 - Z₃
1234 - 6 - 6 - 24P₃ - K
LU₅₈ - 58 - R₁S₂ - 1234
T₂ - 91 - 1 - C
4E₃₃ - 7H - A - 2 - X₁
543D - 1C - F₂ - KL₆ - 1 - W₇

AL-LO	□ □
BOK-KEN-WA-GEN	□ □ □ □
CO-CA-CO-LA	□ □ □ □
DOK-WER-KER	□ □ □
EEN	□
FRUIT-VER-KO-PER	□ □ □ □
GROOT-MOE-DER	□ □ □
HEK-KEN-SPRING-ER	□ □ □ □
IE-MAND	□ □
JAN-DOOM-DOM-DOOR	□ □ □ □
KOM-MER-LOON	□ □ □
LI-MO-NA-DE	□ □ □ □
MO-TOR	□ □
NO-TEN	□ □
DOOR-LOGS-VLOOT	□ □ □ □
PAP-SCHOOL-LO-PER	□ □ □ □
QO-QO-RI-QO	□ □ □ □
RE-YOL-YER	□ □ □

A	▲
B	■
C	■
D	■
E	■
F	■
G	■
H	■
I	■
J	■
K	■
L	■
M	■
N	■
O	■
P	■
Q	▲
R	■

SA-KRI-STIE	□ □ □	S	S
TON	□	T	T
U-NI-FORM	□ □ □	U	U
VER-KEN-NERS-TROEP	□ □ □ □	V	V
WEER-OP-KOMST	□ □ □	W	W
ZON-DER-ZERO	□ □ □ □	X	X
YORK-BLIJFT-TOCH-YORK	□ □ □ □	Y	Y
ZONS-ON-DER-GANG	□ □ □ □	Z	Z

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