Cryptologie

Werkboek van: ……..

Duidelijk Wiskunde

www.DuidelijkWiskunde.nl
DuidelijkWiskunde@gmail.com

Inhoud

Aanwijzingen voor je aan het werk gaat

- Lees alle informatie heel goed. Soms zal je de tekst misschien wel een paar keer moeten lezen voor je goed begrijpt wat er staat.
- Als er een voorbeeld gegeven wordt, kijk dan goed of je begrijpt hoe het gedaan wordt. Ga pas verder als je het voorbeeld snapt.
- Gebruik bij dit werkboekje ruitjespapier (of een ruitjesschrift) zodat je gemakkelijk tabellen kunt maken voor het versleutelen van de codes. In dit werkboekje schrijf je alleen de antwoorden.
- Reken erop dat er regelmatig wat fout zal gaan bij het werken aan het coderen en decoderen. Schrijf daarom met potlood, zodat je fouten gemakkelijk kunt uitgummen.
- Bij sommige opgaven staat een *. Dan staat er achterin dit boekje een tip die je verder kan helpen als je vast zit. Niet te snel kijken, eerst zelf goed proberen!

De leer van geheimschriften

In dit werkboekje leer je over verschillende manieren om berichten zodanig te bewerken dat alleen degene voor wie het bestemd is het kan lezen. De leer over geheimschrift wordt 'cryptologie' genoemd.
Hieronder staan een aantal begrippen die je in dit werkboekje tegenkomt.

Cryptologie	De wetenschap die zich bezig houdt met manieren waarop berichten te vercijferen zijn en codes te ontcijferen of te kraken zijn.
Bericht, klare tekst	Het leesbare bericht dat je wilt overbrengen.
Code, geheimschrift	Het versleutelde bericht dat niet leesbaar is voor mensen die de sleutel niet weten.
Vercijferen, versleutelen, coderen	Drie verschillende woorden die hetzelfde betekenen: een bericht omzetten in code die alleen te lezen is voor degene die de sleutel weet.
Ontcijferen, klaren, decoderen	Drie verschillende woorden die allemaal betekenen: een code weer omzetten naar het bericht met behulp van de sleutel van de code.
Sleutel	Informatie die je nodig hebt om de code weer om te zetten naar het leesbare bericht. Soms is daarvoor een sleutelwoord nodig, soms alleen kennis over de methode die is gebruikt.
Kraken	Zonder de sleutel een code ontcijferen.

Opgave:*

Kraak de volgende code:

9 11 8 15 15 16 4 1 20 10 5 22 5 5 12 16 12 5 26 9 5 18 8 5

. . . . . .

2 20 2 9 10 8 5 20 23 5 18 11 5 14 1 1 14 3 18 25 16 20 15 12

. . . . . .

15 7 9 5.

. . . .

Polybiusvierkant

Rond 200 voor Christus leefde de Griekse historicus Polybius. Hij gebruikte een vorm van cryptografie waarbij elke letter door twee cijfers wordt vervangen.

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	YZ

Het Polybiusvierkant

Het Polybiusvierkant heeft een vakje te weinig voor het Nederlandse alfabet. Het Griekse alfabet dat Polybius gebruikte heeft 24 letters en dan past het natuurlijk wel. Toch is het niet erg, want als je een bericht leest waar het woord YATERDAG in staat, kun je vast wel bedenken dat de eerste letter niet de Y maar de Z moest zijn.

Van bericht naar code:

Voor het vercijferen van een tekst zet je elke letter om in twee coördinaten: eerst het rijnummer en dan het kolomnummer.

Het woord	V	I	E	R	K	A	N	T
wordt dan	52	24	15	43	31	11	34	45

Opgaven:

1. * Ontcijfer de volgende code met het Polybiusvierkant:

   32 15 45 45 15 43 44 53 35 43 14 15 34 13 24 25 21 15 43 44

   . . . .

2. Vercijfer met het Polybiusvierkant:

   W A A R O N T M O E T I K J O U?

   . . . .

3. Bij het coderen moet je eerst het nummer van de rij, en dan het nummer van de kolom gebruiken. Soms gaat dat wel eens mis en worden de cijfers omgedraaid. In onderstaande code zitten een paar van dat soort foutjes. Kun je de boodschap toch ontcijferen?

   44 45 11 35 33 55 15 44 51 51 43 53 41 14 15 23 35 51 31 52

   . . . .

   11 34 41 15 44 45 43 11 11 45.

   . . . .

Zigzag Code

Er zijn geheimschriften waarbij de letters van het bericht zodanig door elkaar gehusseld worden dat je alleen als je de sleutel weet de letters weer op de goede plek kunt zetten. Deze codes worden **transposities** genoemd, dat betekent: van plaats veranderen.

Bij het gebruik van de zigzag code wordt het bericht al zigzaggend over twee regels geschreven, die daarna achter elkaar worden geplakt.

Van bericht naar code:

Bericht: DIT IS NOG MAAR HET BEGIN

Vercijferen:

1. Schrijf het bericht zigzaggend op twee regels onder elkaar.

D		T		S		O		M		A		H		T		E		I	
	I		I		N		G		A		R		E		B		G		N

2. Zet de tweede regel achter de eerste regel.

D	T	S	O	M	A	H	T	E	I	I	I	N	G	A	R	E	B	G	N

3. Schrijf het gecodeerde bericht op in blokken van 4 letters.

Code: DTSO MAHT EIII NGAR EBGN

Opmerkingen:

I. Het is vaak de gewoonte om een code in letterblokken van bijvoorbeeld 4 letters te schrijven.

II. Als het aantal letters van een bericht niet uitkomt, voeg je gewoon een paar onzinletters aan het eind toe. Na het ontcijferen ziet de lezer vanzelf dat deze letters niet bij het bericht horen. Denk erom: de extra letters moet je toevoegen achteraan **het bericht**! Als je het achteraan de code zou toevoegen krijg je je bericht niet meer goed ontcijferd.

Opgaven:

1. Vercijfer het bericht: DIT MAG NIEMAND TE WETEN KOMEN. Schrijf de code in blokken van 5 letters.

   . . . . . .

2. * Voor het ontcijferen van een code, moet je de handelingen **precies achterstevoren** uitvoeren.
   Probeer of dat lukt met de code HTNC JEEI GLKA EOTI FRNS EUTX.
   Schrijf het bericht hieronder.
   Als het niet lukt: kijk bij de tips achterin dit werkboekje!

   . . . . . .

3. Ontcijfer de volgende code: DZKA TSIT ERED GUEE ARIN EMEG LIFW

   . . . . . .

4. Opdracht voor tweetallen: Bedenk allebei een (kort) bericht en vercijfer dat met de zigzagcode. Ontcijfer daarna elkaars code.

   Mijn bericht:

   . . . . . .

   In code is dat:

   . . . . . .

   De code die ik kreeg om te ontcijferen:

   . . . . . .

   Het bericht dat er stond na ontcijferen:

   . . . . . .

Kolomcode

Ook de kolomcode is een transpositie.

Van bericht naar code:

Bericht: RAAK NIET IN DE WAR MET RIJEN EN KOLOMMEN

Vercijferen:

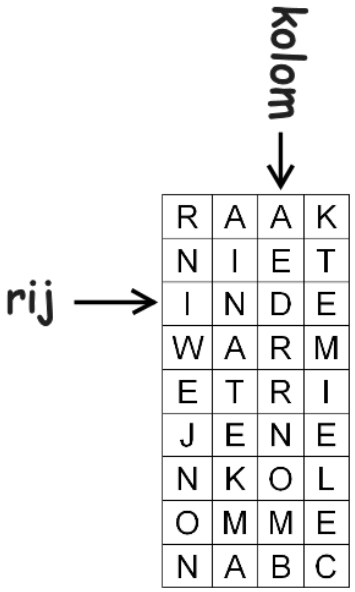
1. Schrijf het bericht in een tabel.
   Schrijf van links naar rechts, en als de rij vol is begin je op de volgende rij. Vul de tabel zo nodig aan met één of meer onzinletters.
2. Schrijf nu de code op door de letters van boven naar beneden te lezen, te beginnen bij de eerste kolom.

R	A	A	K
N	I	E	T
I	N	D	E
W	A	R	M
E	T	R	I
J	E	N	E
N	K	O	L
O	M	M	E
N	A	B	C

Code: RNIW EJNO NAIN ATEK MAAE DRRN OMBK TEMI ELEC

Opmerking:

In een tabel loopt een rij horizontaal,
en een kolom verticaal.



Opgaven:

1. Vercijfer het volgende bericht met een tabel van 4 rijen en 7 kolommen. Gebruik een onzinletter om het aantal letters aan te vullen.

   Bericht: DE BUURVROUW GAAT MORGEN OP REIS

   Code: . . . . . .

2. * Probeer te bedenken hoe je de stappen precies omgekeerd kunt uitvoeren om onderstaande code te ontcijferen. Er is een tabel van 7 rijen en 4 kolommen gebruikt.

   Code: DDST ETSE DTTN HALE AEHU BARA GEIC

   Bericht: . . . . . .

3. Ontcijfer de volgende code met een tabel van 3 rijen en 8 kolommen.

   Code: WGEO ABEA ENTU SHRD EEAT NGGL

   Bericht: . . . . . .

4. * Van de volgende tekst weet je niet welke tabel er bij hoort. Kun je hem toch ontcijferen? Tip: Bedenk in wat voor tabel de letters zouden passen.

   Code: EEERE UINTS SEGLL

   Bericht: . . . . . .

5. Nog een kolomcode zonder dat je de tabel weet. Lukt deze ook?

   Code: DINER HAKED ETELH LTUAB IAOSR VCCER

   Bericht: . . . . . .

Kolomcode met sleutelwoord

Bij een Kolomcode met sleutelwoord worden de letters nog iets meer door elkaar gegooid. Na het opschrijven van het bericht in de tabel wisselen de kolommen van plaats. Dat gebeurt door middel van een sleutelwoord.

Van bericht naar code:

Bericht: HET AVONDETEN IS BIJNA KLAAR
Sleutelwoord: trap

Vercijferen:

1. Maak een tabel waarin je bovenin het sleutelwoord schrijft. Het aantal kolommen is dus net zoveel als het aantal letters van het sleutelwoord.

2. Schrijf het bericht in de tabel. Schrijf van links naar rechts, en als de rij vol is begin je op de volgende rij.

t	r	a	p
H	E	T	A
V	O	N	D
E	T	E	N
I	S	B	I
J	N	A	K
L	A	A	R

⇨

a	p	r	t
T	A	E	H
N	D	O	V
E	N	T	E
B	I	S	I
A	K	N	J
A	R	A	L

3. Verwissel de kolommen van plaats. Doe dat zo dat de letters van het sleutelwoord op alfabetische volgorde komen te staan.

4. Schrijf de code op door de letters van boven naar beneden te lezen, te beginnen bij de eerste kolom.

Code: TNEB AAAD NIKR EOTS NAHV EIJL

Opmerkingen:

I. Bij het ontcijferen moet je de 4 stappen in omgekeerde volgorde uitvoeren, dus eerst stap 4, dan stap 3 enz.
II. Elk van die vier stappen moet je ook in omgekeerde volgorde uitvoeren!

Opgaven:

1. Vercijfer het volgende bericht met een tabel van 5 rijen en 4 kolommen. Gebruik het sleutelwoord 'hond'. Gebruik een onzinletter om het aantal letters aan te vullen.

   Bericht: DE COMPUTER IS GEHACKT

   Code: . . . . . .

2. * Ontcijfer onderstaande code. Lees goed de opmerkingen op pagina 12 voor je aan de slag gaat.

   Code: EJOE DDPB RFEL OEET DITG NVSE sleutelwoord 'kundig'

   Bericht: . . . . . .

3. Ontcijfer de volgende code. Het sleutelwoord is: 'stoep'

   Code: REEVA VTHER RGEEN EGSDI FURIE NTUTN

   Bericht: . . . . . .

4. * De volgende code is vercijferd met een onbekend sleutelwoord. Je weet wel dat die sleutel 3 letters lang is. Kun je het bericht ontcijferen?

   Code: EDE TLT NMR HRF EEC EIV

   Bericht: . . . . . .

5. * Waarom is het sleutelwoord 'acht' niet zo'n gelukkige keus?

   Antwoord: ……

   ……

6. Waarom kun je het woord 'twee' niet als sleutelwoord gebruiken?

   Antwoord: ……

   ……

Caesar-Code

Geheimschriften waarbij letters vervangen worden door andere letters, of door cijfers, worden **substituties** genoemd. Substitutie betekent: vervangen. Bij een **mono-alfabetische substitutie** (mono betekent: één) wordt elke letter altijd door hetzelfde andere symbool (letter of cijfer) vervangen. Verderop in dit boekje maak je ook kennis met **poly-alfabetische substituties** (poly betekent: veel), waarbij een letter niet altijd door hetzelfde symbool wordt vervangen.

Julius Caesar gebruikte rond 50 v Chr. een code waarbij elke letter vervangen werd door de letter die 3 plaatsen verderop in het alfabet staat. Zo werd de A een D, de B een E, de C een F, enz. En (logischerwijze) de X wordt de A, de Y wordt de B en de Z wordt de C. Dit wordt de C^3 (Caesar-3) code genoemd.
Bij de C^7 code worden de letters vervangen door letters die 7 plaatsen verderop staan.

Van bericht naar code:

Bericht: DIT IS NIET ZO MOEILIJK (C^3)

Vercijferen:

D	I	T	I	S	N	I	E	T	Z	O	M	O	E	I	L	I	J	K
+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
G	L	W	L	V	Q	L	H	W	C	R	P	R	H	L	O	L	M	N

Code: GLWL VQLH WCRP RHLO LMN

Opmerking:

I. Om een Caesar-code te kunnen ontcijferen kan het handig zijn om even twee keer het alfabet onder elkaar op te schrijven, waarbij de tweede rij het benodigde aantal plaatsen verschoven is.

II. Soms weet je wel dat een tekst met een Caesar-code is vercijferd, maar niet met welke Caesar-code. Met wat meer moeite kun je dan ontdekken welke Caesarcode je moet gebruiken.
- 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 'B', 'B' wordt 'C', enzovoorts.
- Herhaal dit totdat je een regel krijgt met normale leesbare tekst. Je weet nu hoever je de letters moet verschuiven om het bericht te kunnen lezen.

Opgaven:

1. Vercijfer de volgende tekst met de C^5-code.

   Bericht: KIJK UIT NAAR EEN GROENE AUTO

   Code: . . . . . .

2. * Ontcijfer de volgende code:

   Code: QSVKI RMWIV AIIVI IRHEK (C^4)

   Bericht: . . . . . .

3. Hieronder staat een gecodeerd bericht met de C^{24}-code. Je kunt het dus ontcijferen door elke letter '-24' te doen. Kan dat ook handiger?

   Code: ECCD KGHK YYPQ JYEP MMKR YYPR

   Bericht: . . . . . .

Soms weet je wel dat een tekst met een Caesar-code is vercijferd, maar niet met welke Caesar-code. Hieronder wordt beschreven hoe je die code dan kunt kraken.

- Schrijf het eerste woord (of bijvoorbeeld de eerste tien letters) bovenaan een leeg blaadje.
- Schrijf eronder dezelfde tekst, met alle letters 'één letter verder'. 'A' wordt 'B', 'B' wordt 'C', enzovoorts.
- Herhaal dit totdat je een regel krijgt met normale leesbare tekst. Je weet nu hoever je de letters moet verschuiven om het bericht te kunnen lezen.

4. Bij de volgende code weet je niet om welke Caesar-code het gaat. Probeer de code te kraken op de manier zoals hierboven beschreven staat.

   Code: CEQC FALU UAYY HEIJ DYEI ZZCY

   Bericht: . . . . . .

5. Met welke Caesarcode is het bericht van opgave 4 versleuteld?

Substitutie met sleutelwoord

Omdat er maar een beperkt aantal Caesar-codes zijn, zijn die niet zo moeilijk te kraken. Je kunt natuurlijk ook op andere manieren letters vervangen door letters.

Bij 'substitutie met sleutelwoord' maak je een tabel waarmee je elke letter kunt vervangen door een andere letter. Iedereen die het sleutelwoord weet, kan dezelfde tabel maken en de gecodeerde letters weer vervangen door de letters van het bericht.

Van bericht naar code:

Neem het sleutelwoord: vliegvakantie

1. Schrijf het alfabet op een rij.

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

2. Schrijf daaronder de letters van het sleutelwoord achter elkaar, waarbij je letters die je al gehad hebt overslaat.

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
V	L	I	E	G	A	K	N	T																	

3. Ga na de laatste letter van het sleutelwoord door met de letter die daarna in het alfabet aan de beurt is. Als laatste letter had je net 'T' opgeschreven, dus ga je nu verder met U. Je slaat letters die je al gehad hebt over.
   De letter V zat al in het sleutelwoord dus die heb je al gehad. Daarom schrijf je na de U de W, X, Y en Z op. Na 'Z' begin je weer bij 'A' (maar omdat die al in het sleutelwoord zat sla je die in dit geval over en schrijf je de 'B' op) en zo ga je verder tot alle letters geweest zijn.

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

4. Door de letters van je bericht in de bovenste rij op te zoeken en te vervangen door de letters die eronder staan versleutel je je bericht.

Opgaven:

1. Ontcijfer de code hieronder met het sleutelwoord VLIEGVAKANTIE

   Code: EGJT UEOX TGKJ OBBF LTUQ

   Bericht: . . . . . .

2. Maak een versleuteltabel met het sleutelwoord SCHOOLBOEKEN en versleutel het volgende bericht.

   Bericht: HET ALARM STAAT UIT

   Code: . . . . . .

3. * Ontcijfer de volgende code. Het sleutelwoord is BUREAUSTOEL.

   Code: MBVH AADE ARWE ALKW

   Bericht: . . . . . .

4. * Waarom is het woord 'ZAND' geen geschikt sleutelwoord?

   Antwoord: ……

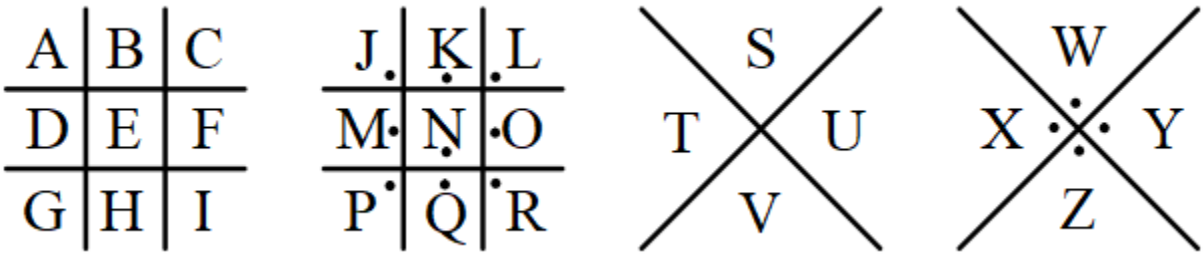
   ……

Geheimschrift van de vrijmetselaars

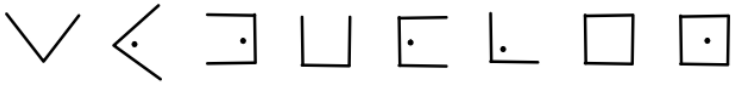
In de 16e eeuw werd er door een geheim broederschap (de rozenkruisers) een geheimschrift bedacht dat later ook door de vrijmetselaars werd gebruikt en daardoor bekend is geworden als het geheimschrift van de vrijmetselaars.

Van bericht naar code:

Bij deze versleuteling wordt elke letter door een symbool weergegeven:



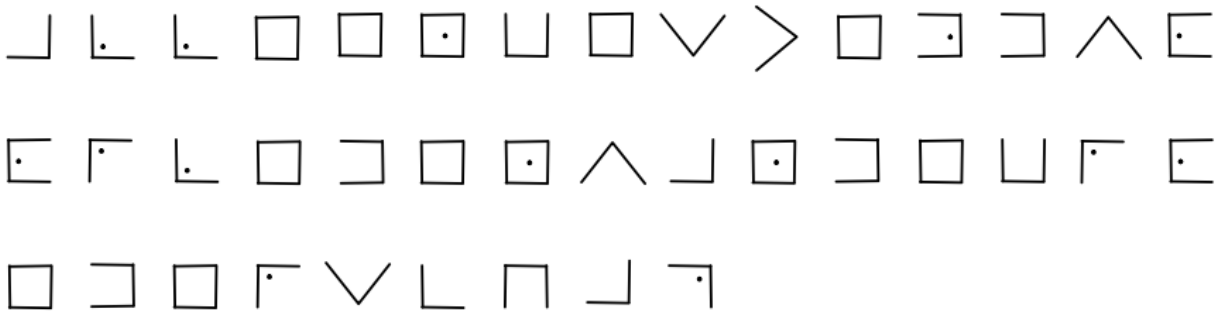
Het woord SYMBOLEN wordt dan:



Deze vorm van geheimschrift valt ook onder de mono-alfabetische substituties, omdat elke letter telkens door hetzelfde symbool wordt weergegeven.

Opgaven:

1. Kun je ontcijferen wat hier staat?



2. Er wordt een wachtwoord doorgegeven met behulp van de vrijmetselaarscode. Degene die de code heeft opgeschreven is vergeten om punten in de symbolen te zetten waar dat zou moeten. Kun je toch proberen of je het wachtwoord kunt ontcijferen?

3. Als een wachtwoord 4 letters zou hebben, en de punten zouden vergeten zijn, hoeveel verschillende mogelijkheden zou je dan moeten opschrijven om te kijken welk wachtwoord het kan zijn?

   Antwoord: ……

Frequentie-analyse

Een code die ontstaan is via het vervangen van letters waarbij elke codeletter altijd voor dezelfde berichtletter staat kun je proberen te kraken met 'frequentie-analyse'. Het woord 'frequentie' betekent: 'hoe vaak iets voorkomt'. En 'analyse' betekent: onderzoeken.
Door te onderzoeken welke codeletters vaak voorkomen in de code, kun je proberen te raden welke berichtletters het zouden moeten zijn.
In de tabel hieronder zie je hoe vaak een letter gemiddeld voorkomt in een Nederlandse tekst van 1000 letters lengte.

A	B	C	D	E	F	G	H	I	J	K	L	M
74	15	14	59	192	7	33	28	60	12	22	39	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
102	58	15	1	61	37	65	16	27	17	1	7	16

De manier waarop je stap voor stap het kraken met behulp van frequentie-analyse kunt aanpakken wordt hierna uitgelegd met behulp van een voorbeeld.

Voorbeeld:

X K   M G   E A G L D G K V X G V Z T G U   H D K   N G

. .   . .

P G I Z H H G U X N H   Y X G K   F C G   S Z Z H   M G   U G V V G A B

. . . .

Z   G K   K   X K   M G   K G M G A U Z K M B G   V Z Z U

.   . .   .

P G T A D X H V   O C A M G K

. . . .

Als je telt hoe vaak elke letter voorkomt in de code krijg je het volgende resultaat.

codeletter	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
frequentie	5	2	2	3	1	1	20	6	1	0	10	1	6	2	1	2	0	0	1	2	5	6	0	6	1	8
berichtletter																										

De letter G komt het vaakst voor en zal waarschijnlijk voor de E staan. Dat kun je dus in de tabel invullen. Gebruik potlood, want je weet het natuurlijk nog niet zeker! Vul ook onder elke letter R in de code de E in.

De volgende letter die het vaakst voorkomt in de code is de letter K. De kans is groot dat dat de N voorstelt.

Het woordje 'de' gebruiken we vaak. In de code komt MG drie keer voor, en de G is de E weten we al. We weten nu dus ook welke letter voor de D zal staan.

De letter A komt in het Nederlands op de derde plaats. In de code komt de letter Z op de derde plaats. Wel even uitproberen of de woorden die je dan krijgt kunnen kloppen.

Opgaven:

1. * Maak het kraken van code af. Bij de tips staan nog een paar letters gegeven.

2. * Kraak ook de volgende code met frequentie-analyse. Een paar letters krijg je al:

S H V K Z S H P K K A C H H R F S H W H A D N C F H Z

. . . .

L K Z S H N T B B K Z S K Z F G I Z Z H Z T Z F N D O R H A H Z

. . . .

T B S K F C D O S H X P H I F H P L K Z S H N T S H V D X F

. . . .

codeletter	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
frequentie																										
berichtletter						T						V										W				

3. Waarom is een heel kort bericht lastig te kraken met frequentie-analyse?

   Antwoord: ……

   ……

4. * Het volgende bericht zal ook lastig te kraken zijn met frequentie-analyse. Waarom?

   Ik kom thuis om acht uur. Daarna ga ik naar dat park naast Tivoli. Ik hoop dat jij ook komt. Ik wacht tot twaalf uur op jou.

   Antwoord: ……

   ……

Vigenère-methode

De Franse diplomaat en cryptograaf Vigenère beschreef in 1586 een manier van het vervangen van letters die niet te kraken leek. Hoewel de methode niet door hemzelf bedacht was, wordt het toch de Vigenèremethode genoemd.

Bij deze methode van vercijferen worden letters ook weer door andere letters vervangen, maar niet elke keer door dezelfde letter. Deze methode hoort daarom bij de **'poly-alfabetische substituties'**.

Van bericht naar code:

We versleutelen het woord : TWEEDE en gebruiken het sleutelwoord 'voet':

1. Schrijf TWEEDE boven in een tabel.
2. Schrijf op de rij eronder het sleutelwoord 'voet' telkens achter elkaar.
3. Schrijf onder elke letter van het sleutelwoord de hoeveelste letter van het alfabet het is.
   De v is de 22e letter van het alfabet, daarom komt daar 22 te staan, de o is de 15e letter, dus komt daar 15 te staan, enz.
4. De letters van de code kun je vinden door de letters van het bericht zoveel te verplaatsen als het getal eronder aangeeft.
   De eerste letter T moet 22 plaatsen verschuiven. Als je bij de Z bent aangekomen tel je daarna verder bij de A, B, enzovoorts. De letter T wordt vervangen door de P, want die ligt 22 plaatsen verder (tel maar even na).

bericht	T	W	E	E	D	E
sleutelwoord	v	o	e	t	v	o
verplaatsing	22	15	5	20	22	15
code	P					

Opgave:

1. Vercijfer op deze manier de volgende twee letters (W en E) van het bericht.

Je hebt gemerkt dat er heel wat telwerk komt kijken bij deze manier van versleutelen. Daarom is er een tabel gemaakt waarin het wat sneller gaat: de Vigenère-tabel.

		Letters van het bericht																									
		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**
Rijen met de letters en nummer van het sleutelwoord	**1** **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	A
	2 **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	A	B
	3 **c**	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
	4 **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	D
	5 **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	D	E
	6 **f**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	7 **g**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	8 **h**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	9 **i**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	10 **j**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	11 **k**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	12 **l**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	13 **m**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	14 **n**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	15 **o**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	16 **p**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	17 **q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	18 **r**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	19 **s**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	20 **t**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	21 **u**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	22 **v**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	23 **w**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	24 **x**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	25 **y**	Z	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
	26 **z**	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

Belangrijk:

- De letters van het bericht staan bovenaan;
- De letters van het sleutelwoord, met bijbehorend getal dat aangeeft hoeveel verplaatsingen er gedaan moeten worden, staan links;
- De letters van de code staan in het grote middenvak.

Vercijferen:

1. Zoek de letter die je wilt vercijferen op de bovenste rij van de tabel bij de 'berichtletters'. Bijvoorbeeld de eerste letter T van het bericht.
2. Kijk welke letter van het sleutelwoord erbij hoort en zoek aan de linkerkant de rij die hoort bij bij die letter.
   Onder de letter T staat de sleutelletter v. Je hebt daarom rij 22 van de tabel nodig.
3. De codeletter vind je op het kruispunt van de kolom onder de berichtletter (T) met de rij van de sleutelletter (v). Als je daar kijkt zie je in dit geval de letter P.

Opgave:

2. * Maak het vercijferen van het woord TWEEDE af. Door welke letters worden de drie letters E vervangen?

   Antwoord: ……

Van code naar bericht:

Bij het ontcijferen doe je alle stappen precies andersom. Als je de code ZJZOEMC wilt ontcijferen met sleutelwoord 'val' schrijf je eerst de code op en het sleutelwoord met het bijbehorende getal erboven.

bericht							
sleutelwoord	v	a	l	v	a	l	v
verplaatsing	22	1	12	22	1	12	22
code	Z	J	Z	O	E	M	C

Ontcijferen (je moet alle stappen precies omgekeerd doen):

1) Kijk op welke rij je moet zijn.
   Voor de eerste letter is dat op rij 22, van de sleutelletter v.
2) Zoek op die rij de codeletter die je weet.
   Je zoekt dus op rij 22 de letter Z.
3) Kijk welke letter helemaal bovenaan staat in de kolom van die codeletter.
   Helemaal boven de Z die we net gevonden hebben staat de D.
4) Deze letter is de letter van het bericht.
   De eerste letter van het bericht is een D.

Opgave:

3. * Maak het ontcijferen van de code in bovenstaande tabel af.

Vigenère en een klaarautoclaaf

In het woord 'Klaarautoclaaf' zitten drie woorden:

- klaar komt van 'klaren', je 'klaart' een tekst.
- auto komt van autos (latijn) en betekent 'zelf'.
- claaf ook uit het latijn en betekent 'sleutel'.

Met een klaarautoclaaf begin je met een sleutelwoord, en nadat je dat éénmaal gebruikt hebt onder het bericht, gebruik je de letters van het bericht verder als sleutel.

Van bericht naar code:

Bericht: GEBRUIK HET BERICHT ALS SLEUTEL
Sleutel: 'bos'

Vercijferen:
Het bericht hieronder wordt vercijferd met de Vigenère-tabel. De eerste drie letters met behulp van de sleutel, de volgende letters met de letters van het bericht zelf.

bericht	G	E	B	R	U	I	K	H	E	T	B	E	R	I	C	H	T	A	L	S	S	L	E	U	T	E	L
sleutel	b	o	s	g	e	b	r	u	i	k	h	e	t	b	e	r	i	c									
verplaatsing	2	15	19	7	5	2	18	21	10	11	8	5	20	2	5	18	9	3									
code	I	T	U	Y	Z	K	C	C	N																		

Van code naar bericht:

Code: GJQS YIFO RJZQ KL
Sleutel: 'jacht'

bericht	W	I	N											
sleutel	j	a	c	h	t	w	i	n						
verplaatsing	10	1	3	8	20	23	9	14						
code	G	J	Q	S	Y	I	F	O	R	J	Z	Q	K	L

1. Neem de rij die bij de letter van de sleutel hoort.
   In bovenstaand voorbeeld is dat bij de eerste letter ('J') de 10e-rij.
2. Zoek in die rij de letter die je in de code aantreft. (Bijv. de letter 'G' uit het voorbeeld)
3. Kijk welke letter boven de kolom staat. (Helemaal bovenaan de kolom waar je de G gevonden hebt staat de W). Dat is de letter van het bericht.
4. De eerste 5 letters van de code kun je met het sleutelwoord ontcijferen.
   Voor de volgende letters gebruik je de letters van het bericht die je al ontcijferd hebt.

Opgaven:

1. Maak het vercijferen van het bericht ' GEBRUIK HET BERICHT ALS SLEUTEL ' dat op de vorige bladzijde staat af.

2. * Maak het ontcijferen van het bericht op de vorige bladzijde af.

3. * Ontcijfer onderstaande tekst, waarbij als beginsleutel het woord 'auto' is gebruikt.

   Code: PIXT GRIA ANKZ NCZI JGRL

   Bericht: . . . . . .

ADFGVXcode

In de Eerste Wereldoorlog werd door de Duitsers een geheimschrift gebruikt waarbij elke letter eerst vervangen wordt door twee andere letters, en vervolgens nog door elkaar gegooid met een kolomverschuiving op een manier zoals we bij 'kolomcode met sleutelwoord' hebben gezien. Er wordt dus eerst 'substitutie' en dan 'transpositie' gebruikt.

Er wordt gebruik gemaakt van een tabel met alle 26 letters, en 10 cijfers. De letters en cijfers worden willekeurig in de tabel gezet: belangrijk is dus dat degene voor wie het bericht bestemd is deze tabel ook heeft.

	A	**D**	**F**	**G**	**V**	**X**
A	R	G	7	M	C	3
D	K	D	4	I	9	T
F	X	S	A	1	Z	H
G	8	Q	Y	J	0	P
V	O	B	2	L	U	E
X	5	W	N	F	6	V

In de vercijfertabel worden de letters van het bericht vervangen door de letter aan de linkerkant van de rij, en aan de bovenkant van de kolom waarin ze staan.

Met de tabel hiernaast wordt de K vervangen door DA en de L door VG.

De letters ADFGVX verschillen in het morse-alfabet veel van elkaar. In de tijd dat dit geheimschrift werd gebruikt werden berichten meestal via morse verstuurd. Door voor deze letters te kiezen in deze code was de kans op fouten bij het versturen kleiner.

Van bericht naar code.

Bericht: STUUR VERSTERKING (met sleutelwoord 'dorpje')

Stap 1: omzetten met de ADFGVXtabel.

S T U U R V E R S T E R K I N G

FD DX VV VV AA XX VX AA FD DX VX AA DA FG XF AD

Stap 2:
Schrijf de letters in een tabel met het sleutelwoord dorpje. De tabel krijgt dus 6 kolommen.
Voer daarna een kolomverschuiving uit zoals bij 'kolomcode met sleutelwoord'.

d	o	r	p	j	e
F	D	D	X	V	V
V	V	A	A	X	X
V	X	A	A	F	D
D	X	V	X	A	A
D	A	F	G	X	F
A	D	G	V	V	F

⇨

d	e	j	o	p	r
F	V	V	D	X	D
V	X	X	V	A	A
V	D	F	X	A	A
D	A	A	X	X	V
D	F	X	A	G	F
A	F	V	D	V	G

Code: FVVD DAVX DAFF VXFA XVDV XXAD XAAX GVDA AVFG

Opgaven:

1. * Ontcijfer met behulp van de gegeven ADFGVX-tabel en het sleutelwoord 'urgent' de volgende code:

   Code: AADA VADV VFDG XAFD AFGX XAFF.

   Bericht: . . . . . .

2. Je vervangt bij deze code elke letter telkens door dezelfde twee letters uit de ADFGVX-tabel. Toch kun je hier geen frequentie-analyse toepassen. Waarom niet?

   Antwoord: ……

   ……

3. Waar moet je op letten bij het kiezen van een sleutelwoord? Bedenk een sleutelwoord dat wel geschikt is, en ook een sleutelwoord dat niet geschikt is.

   Antwoord: ……

   ……

   ……

   ……

RSA-code

Bij de codes die we tot nu toe bekeken hebben bestaat altijd het probleem dat iemand misschien afluistert als je de sleutel doorgeeft. Met de communicatie via telefoon en internet is het soms moeilijk om zeker te weten dat er niemand stiekem meeluistert.

In de tijd dat internet ontstond waren er cryptografen, informatici en wiskundigen die bedachten dat je met het gebruik van wiskundige formules samen kunt overleggen over een sleutel zonder dat degene die dat overleg afluistert daarna weet wat de sleutel is. En, mooier nog, er kan een sleutel doorgegeven worden waarmee iedereen een bericht kan versleutelen om aan jou te sturen, zonder dat met diezelfde sleutel de code weer ontcijferd kan worden. Daar is een andere sleutel voor nodig die jij alleen weet.

Bij de RSA-code heb je twee sleutels: een openbare sleutel en een geheime sleutel. Als je de openbare sleutel weet kun je wel berichten versleutelen, maar je kunt dat proces niet eenvoudig omkeren en de code weer ontcijferen.

De naam RSA verwijst naar de eerste letters van de namen van de personen die deze code in 1977 hebben bedacht: Ron **R**ivest, Adi **S**hamir en Leonard **A**dleman. De RSA-code wordt nu nog steeds gebruikt bij het beveiligen van bijvoorbeeld je bankpasje.

De RSA-code maakt gebruik van het feit dat het niet zo moeilijk is om twee priemgetallen te vermenigvuldigen met elkaar, maar dat het heel moeilijk is om die twee priemgetallen te vinden als je alleen het antwoord van de vermenigvuldiging, het product, weet.

> **Definitie**
> Een priemgetal is een positief geheel getal met precies twee delers, namelijk 1 en zichzelf.

Opgaven:

1. Lees de definitie van een priemgetal. Wat is het kleinste priemgetal?

   Antwoord: ……

2. Schrijf alle priemgetallen op die kleiner dan 100 zijn.

   Antwoord: ……

   ……

   ……

3. Bereken het product van de volgende priemgetallen. Schrijf hier alleen het antwoord op.

   a. 13 x 131 = …….

   b. 17 x 149 = …….

   c. 41 x 251 = …….

4. De volgende getallen zijn producten van twee priemgetallen. Probeer te ontdekken welke priemgetallen dat zijn.

   a. 377 = ……. x …….

   b. 1403 = ……. x …….

   c. 1829 = ……. x …….

Waarschijnlijk heb je wel gemerkt dat het zoeken van de twee priemgetallen, als je het product weet, vele malen moeilijker is dan het vermenigvuldigen van twee priemgetallen. Bij opgave 4 ging het om producten met 3 of 4 cijfers.
Bij de RSA-code gaat het om producten met meer dan 1000 cijfers. Zelfs met de krachtigste computers die nu bestaan duurt het dan veel te lang om de bijbehorende priemgetallen te vinden.

Om te begrijpen hoe de RSA-code precies werkt heb je een paar jaar langer wiskunde nodig. In de bovenbouw van het vwo heb je waarschijnlijk voldoende kennis om je daar nog eens in te verdiepen als je het leuk vindt.

Wat vind jij?

Je hebt in dit boekje kennis gemaakt met heel wat coderingssystemen. Op de ruimte hierna schrijf je een stukje over wat jouw mening is over de verschillende geheimschriften.
Denk bijvoorbeeld na over de volgende vragen:
Welk geheimschrift(en) vind je heel goed en waarom?
Welk geheimschrift(en) vind je niet zo goed en waarom niet?
Als je zelf een geheimschrift wilt gebruiken, kies je dan vooral voor veiligheid of voor gemak van gebruiken of verschilt dat per situatie? Waarom?
Welk geheimschrift vind je geschikt om te gebruiken als je berichten naar je klasgenoot wilt sturen die niemand mag lezen, en welk geheimschrift niet? Waarom?

Het maakt niet uit **wat** jouw mening is, maar het maakt wel uit of je kunt uitleggen **waarom** het jouw mening is.

Mijn mening:

……

……

……

……

……

……

……

……

……

……

……

Tips

Blz 5 (opgave)
Wat is het hoogste getal dat in de code staat? Hoe zou je letters op een eenvoudige manier kunnen omzetten in getallen van 1 t/m ….?

Blz 7 (opgave 1)
Het eerste cijfer zoek je aan de linkerkant van het Polybiusvierkant, het tweede cijfer aan de bovenkant. Op het kruispunt vind je de letter. Het getal 32 staat dus voor de L.

Blz 9 (opgave 2)
1. Splits de code eerst in twee gelijke delen.
2. Schrijf het eerste deel op met steeds een leeg vakje tussen de letters.
3. In de open vakjes schrijf je de letters van het tweede deel.

Blz 11 (opgave 2)
Het ontcijferen gaat als volgt:
1. Maak een tabel zoals aangegeven, dus 7 rijen en 4 kolommen. Denk eraan dat een rij van links naar rechts loopt, en een kolom van boven naar beneden!
2. Schrijf dan de code van boven naar beneden. Je begint in de eerste kolom en als die vol is ga je in de tweede kolom verder.
3. Nu kun je het bericht van links naar rechts lezen.

Blz 11 (opgave 4)
De code bestaat uit 15 letters. Je kunt dus een tabel van 3 rijen en 5 kolommen maken, of een tabel van 5 rijen en 3 kolommen. Dat zijn maar twee mogelijkheden die je eenvoudig even allebei kunt uitproberen. Bij één van beiden zal je het bericht kunnen lezen.

Blz 13 (opgave 2)
Het stappenplan voor het ontcijferen gaat als volgt:
1. Het sleutelwoord is 'kundig' dus je moet een tabel met 6 kolommen maken. De code bestaat uit 24 letters, dus je hebt 4 rijen nodig (want 4 x 6 = 24).
2. Schrijf de letters van het sleutelwoord op alfabetische volgorde boven in de tabel.
3. Schrijf de letters van de code van boven naar beneden in de tabel. Je begint in de eerste kolom, als die vol is ga je verder in de tweede kolom, enz.
4. Verwissel de kolommen van plek zodat de letters van het sleutelwoord op de goede plek komen te staan het woord 'kundig' vormen'.
5. Lees nu het bericht van links naar rechts.

Blz 13 (opgave 4)
Op hoeveel verschillende manieren zou je drie kolommen van plaats kunnen laten veranderen? Dat zijn er niet zo heel veel. Je kunt het dus gewoon uitproberen.

Blz 13 (opgave 5)
Wat gebeurt er als je de letters van het sleutelwoord 'acht' op alfabetische volgorde zet?

Blz 15 (opgave 2)
Als een bericht met C^4 versleuteld wordt, verschuift de A naar de …….
Als de code daarna ontcijferd moet worden, verschuift de E terug naar de ……
Dus om een code te ontcijferen moet je niet +4 doen, maar -4!

Blz 17 (opgave 3)
Denk eraan dat je elke letter van het sleutelwoord maar één keer opschrijft in de tabel.
Je tabel komt er dus zo uit te zien:

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

Blz 17 (opgave 4)
Maak eens een versleuteltabel met het woord 'ZAND' als sleutelwoord. Wat valt je op?

Blz 21 (opgave 1)
Tip 1: Het woord NEDE . . AND . E moet NEDERLANDSE worden.
Tip 2: De E staat voor de F, de L staat voor de Q en de D staat voor de U.

Blz 21 (opgave 2)
Tip 1: Zoek eerst uit welke letter de E zal zijn, en daarna de N. Kijk daarna of je weet welke woordjes 'DE' zullen betekenen.
Tip 2: A=R, D=I, N=C.

Blz 22 (opgave 4)
Welke letter komt gewoonlijk het meest voor? Hoe zit dat in deze tekst?

Blz 25 (opgave 2)

De E op de rij van de t (verschuiving 20) geeft een Y.

Rijen met de letters en nummer van het sleutelwoord		Letters van het bericht																									
		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**
1	**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	A
2	**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	A	B
3	**c**	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
4	**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	D
5	**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	D	E
6	**f**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	**g**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	**h**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	**i**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	**j**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	**k**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	**l**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	**m**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	**n**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	**o**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	**p**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	**q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	**r**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	**s**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	**t**	U	V	W	X	**Y**	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	**u**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	**v**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	**w**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	**x**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	**y**	Z	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
26	**z**	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

Blz 25 (opgave 3)

De codeletter Z moet je zoeken op rij nummer 22. Bovenaan staat dan berichtletter D.

Rijen met de letters en nummer van het sleutelwoord		Letters van het bericht																									
		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**
1	**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	A
2	**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	A	B
3	**c**	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
4	**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	D
5	**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	D	E
6	**f**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	**g**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	**h**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	**i**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	**j**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	**k**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	**l**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	**m**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	**n**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	**o**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	**p**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	**q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	**r**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	**s**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	**t**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	**u**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	**v**	W	X	Y	**Z**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	**w**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	**x**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	**y**	Z	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
26	**z**	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

Zie volgende pagina voor nog twee letters van deze code.

De codeletter J moet je zoeken op rij nummer 1. Bovenaan staat dan berichtletter I.

		Letters van het bericht																								
		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**
Rijen met de letters en nummer van het sleutelwoord	1	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	A
	2	**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	A	B
	3	**c**	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
	4	**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	D
	5	**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	D	E
	6	**f**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	7	**g**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	8	**h**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	9	**i**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	10	**j**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	11	**k**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	12	**l**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	13	**m**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	14	**n**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	15	**o**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	16	**p**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	17	**q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	18	**r**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	19	**s**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	20	**t**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	21	**u**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	22	**v**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	23	**w**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	24	**x**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	25	**y**	Z	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
	26	**z**	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

De codeletter Z moet je zoeken op rij nummer 12. Bovenaan staat dan berichtletter N.

		Letters van het bericht																								
		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**
Rijen met de letters en nummer van het sleutelwoord	**1**	**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	A
	2	**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	A	B
	3	**c**	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
	4	**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	D
	5	**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	D	E
	6	**f**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	7	**g**	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	8	**h**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	9	**i**	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	10	**j**	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	11	**k**	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	12	**l**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	**Z**	A	B	C	D	E	F	G	H	I	J	K	L
	13	**m**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	14	**n**	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	15	**o**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	16	**p**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	17	**q**	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	18	**r**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	19	**s**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	20	**t**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	21	**u**	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	22	**v**	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	23	**w**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	24	**x**	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	25	**y**	Z	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
	26	**z**	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

Blz 27 (opgave 2)

bericht	W	I	N	K	E									
sleutel	j	a	c	h	t	w	i	n	k	e				
verplaatsing	10	1	3	8	20	23	9	14	11	5				
code	G	J	Q	S	Y	I	F	O	R	J	Z	Q	K	L

Blz 27 (opgave 3)

Schrijf de code onderin de tabel en het sleutelwoord 'auto' erboven.
Kijk op de rij van de a waar de letter P staat. Kijk dan welke letter boven die rij staat. Dat is de O. Je weet nu de eerste letter van het bericht.
Als je zo ook de I (op de rij van de u), X (op de rij van de t) en T (op de rij van de o) ontcijfert krijg je een N, D en E. Vervolgens vul je het sleutelwoord aan met de eerste vier letters die je al ontcijfert hebt en kun je verder met het ontcijferen van de G, R, I en A.

bericht	O	N	D	E																
verplaatsing	1	21	20	15																
sleutel	a	u	t	o	o	n	d	e												
code	P	I	X	T	G	R	I	A	A	N	K	Z	N	C	Z	I	J	G	R	L

Blz 29 (opgave 1)

De stappen die je moet uitvoeren zijn de volgende:

1. Maak een tabel met 6 kolommen (want het sleutelwoord 'urgent' heeft 6 letters) en 4 rijen (want de code heeft 24 letters en 24:6=4).
2. Schrijf bovenin de tabel de letters van het sleutelwoord, maar doe dit op alfabetische volgorde!
3. Schrijf de code in deze tabel, van boven naar beneden. Je krijgt dan de volgende tabel (vul zelf de rest van de letters aan).

e	g	n	r	t	u
A			X		
A		F			
					F
	V				

⇨

u	r	g	e	n	t
	X		A		
			A	F	
F					
		V			

4. Schrijf de letters nu over uit de tabel, van links naar rechts. Je krijgt dan:

   . X . A . . . . . A F . F . . . . V . . .

5. Elke twee letters geven een plek aan in de ADFGVX-tabel. De eerste twee letters, XX, geven de plek aan van de V. De volgende twee letters, VA, geven de plek aan van de letter O. Je hebt 24 codeletters, dat worden dus 12 berichtletters. Ontcijfer zo verder alle 12 letters van het bericht.

Voor dit werkboek heb ik me laten inspireren door uitgaven van Vierkant voor Wiskunde.

Doeboek 22: Cryptologie, door Maurice Alberts en Joost Langeveld;
Wisschrift 5: Geheimschrift, door Jantine Bloemhof