

6. Gebruik die informatie vervolgens om een deel van de coördinaten toe te kennen. Vul de aldus gevonden elementen van de klaartekst in, en probeer via identificatie van woorden en het inpassen van de overblijvende mogelijkheden de gehele codeertabel te reconstrueren.
7. Omdat over het algemeen slechts een equivalente optelreeks gevonden wordt, zal de resulterende permutatie niet identiek zijn aan de oorspronkelijke, maar - in samenhang met de benutte optelreeks - daarmee equivalent. Merk na het ontcijferen op hoe bij overeenkomstige woorden in de klaartekst de keuze bij de verdeling van woorden in letters en lettergrepen is benut voor het bemoeilijken van de analyse.

## 5.4 Werkschemas

Bekend is dat de optelreeks tien cijfers bevat. *Daarom begint voor elk cryptogram de bovenste regel met het elfde cijfer, terwijl op de tweede regel het cryptogram bij het eerste cijfer begint en de laatste tien cijfers ontbreken.* De cijfers zijn hier per tien gegroepeerd, omdat gebleken is dat daardoor de kans op fouten bij het goed bepalen van de herhalingen geringer is. Op de regel eronder staat hetzelfde cryptogram minus de laatste tien cijfers. Zodoende staan deze regels precies één periode uit elkaar. *Trek de cijfers op de onderste regel volgens het carryloos rekenen van de bovenste af.* Op deze wijze worden de verschilreeksen verkregen, waarin de herhalingen moeten worden opgespoord.

Om het vele werk wat lichter te maken, is een deel van het werk in deze eerste stap reeds gedaan; voor de eerste drie cryptogrammen zijn de verschilreeksen al ingevuld op de derde regel. Alleen voor het vierde en vijfde cryptogram moeten de verschillen nog worden berekend en ingevuld. Dan kan het zoeken naar de herhalingen beginnen, lastiger dan men op het eerste gezicht zou denken. Start daarom de zoektocht maar met het laatste cryptogram ...

bericht 1:

```
3612136956 1250862704 5987163523 6572744272 3770624125 0801903398
9588251696 3612136956 1250862704 5987163523 6572744272 3770624125
4134985360 8648736858 4737301829 1695681759 7208980953 7131389273
```

```
1147998712 36910
```

```
0801903398 11479
```

```
1346095424 25541
```

bericht 2:

```
0229799276 9532549562 3313303729 9076046371
4202392773 0229799276 9532549562 3313303729
6027407503 9313250396 4881864267 6763743652
```

## bericht 3:

9032052704 2626876458 5325876703 3613210183 35000  
 0820450371 9032052704 2626876458 5325876703 36132  
 9212602433 3694824754 3709000355 8398444480 09978

## bericht 4:

2803478612 6840546271 0401419380 0896625921 5315627136 8857694912  
 4610408351 2803478612 6840546271 0401419380 0896625921 5315627136

.....

5240003731 9026904915 7252176956 2113305158 6513862702 9365174168  
 8857694912 5240003731 9026904915 7252176956 2113305158 6513862702

.....

2267641036 8588433556 3697164892 3541306346 6823744279 0894859668  
 9365174168 2267641036 8588433556 3697164892 3541306346 6823744279

.....

9003993548 6112805672 4103235936 2198051072 7040964758 47260  
 0894859668 9003993548 6112805672 4103235936 2198051072 70409

.....

## bericht 5:

8544883580 9003478631 9026993156 4757549156 1341377957 9329083501  
 4499693568 8544883580 9003478631 9026993156 4757549156 1341377957

.....

2872865605 2281438772 0352858678 1003998712 36910  
 9329083501 2872865605 2281438772 0352858678 10039

.....

Uit de gevonden herhalingen moet een optelreeks worden bepaald. Dat is dan één van de honderd equivalente oplossingen. Omdat meer dan één herhaling kan worden gevonden, is het verstandig om uit beide een oplossing te berekenen. Wanneer het goed gedaan is, wordt tussen alle groepjes van twee cijfers een constant verschil gevonden. Zoals bijvoorbeeld tussen (87 65 99 23 10) en (11 99 23 57 44) het verschil steeds (34 34 34 34 34) is. Dit is van groot belang, omdat bij een verkeerde optelreeks de volgende stap de mist in gaat.

Benut het volgende schema voor het bepalen van het additief uit de encicode van de twee componenten van een herhaling; de ene aan de linkerkant voor de dubbele dikke verticale lijn, de andere aan de rechterkant. Stel het additief voor als ab-cd-ef-gh-ij, waarin elke letter een cijfer van het additief voorstelt. Noteer op de bovenste rij voor elke component van de herhaling deze letters in de juiste vakjes, rekening houdend met de positie van de herhalingen in het cryptogram. De dubbele verticale lijnen herinneren er aan dat het additief een periode van vijf dinomes (is tien cijfers) heeft. Het additief begint in het algemeen voor elke component van de herhalingen op een andere positie, denk daaraan. Vul op de derde rij de cijfers van de encicode in. *Let op, gebruik de cryptogramcijfers van de tweede regel ter plaatse van de herhalingen voor deze bepaling.* Begin nu met de eerste dinome van het additief in de linkertabel op nul te stellen (is al reeds ingevuld in de tabel). Vul de bijbehorende dinome van de klaartekstgroep in op de vierde rij en vul die ook in op de juiste plaats in de rechertabel. Bereken daaruit de dinome van het additief ter plaatse en zet die weer in de tabel aan de linkerkant waardoor weer een dinome van de klaartekst wordt gevonden, enz.

	component-1					component-2				
additief a-j										
additief 0-9	00									
dinome										
encicode										

Als het additief is gevonden, kan het strippen van de encicode beginnen. Daarvoor dient het onderstaande schema. Op de bovenste regel staan de cijfergroepen van het cryptogram (de encicode), ditmaal opgesplitst in de dinomes van de onderliggende vercijfering. *Schrijf de tien gevonden optelgetallen van het additief herhaald op de tweede regel en zet daaronder op de derde regel hun verschil, d.w.z. **trek de onderste van de bovenste af.*** In elk cryptogram is de eerste dinome vercijferd met de eerste dinome van het additief, enz. Uit de vorige stap is natuurlijk bekend geworden wat de eerste cijfers van het additief zijn.

Let op. Het is werkelijk belangrijk om het verschil te nemen en niet de som. Alleen zo (encicode-additief=dinome) vindt men de oorspronkelijke vercijferde klaartekstgroep terug. De reden hiervoor is gelegen in de vier combinaties die mogelijk zijn door de keuze van additief/subtractor en optellen/afrekken. Van die vier combinaties zijn er twee goed en twee fout. (Hier moet men of aftrekken of het complement van de gevonden oververcijfering optellen.)

De laatste stap is het ontcijferen en de daaruit volgende reconstructie van de codeertabel. De onderste regel in het werkschema is bestemd voor het noteren van de klaartekst. Gebruik de blanco codeertabel voor de oplossing. Zet in elke cel de bij die coördinaten behorende klaartekstgroep.

bericht 1:

95 88 25 16 96 36 12 13 69 56 12 50 86 27 04 59 87 16 35 23 65 72 74

.....  
.....  
.....

42 72 37 70 62 41 25 08 01 90 33 98 11 47 99 87 12 36 91

.....  
.....  
.....

bericht 2:

42 02 39 27 73 02 29 79 92 76 95 32 54 95 62 33 13 30 37 29 90 76 04

.....  
.....  
.....

63 71

.....  
.....  
.....

bericht 3:

08 20 45 03 71 90 32 05 27 04 26 26 87 64 58 53 25 87 67 03 36 13 21

.....  
.....  
.....

01 83 35

.....  
.....  
.....

bericht 4:

46 10 40 83 51 28 03 47 86 12 68 40 54 62 71 04 01 41 93 80 08 96 62

.....  
.....  
.....

59 21 53 15 62 71 36 88 57 69 49 12 52 40 00 37 31 90 26 90 49 15 72

.....  
.....  
.....

52 17 69 56 21 13 30 51 58 65 13 86 27 02 93 65 17 41 68 22 67 64 10

.....  
.....  
.....

36 85 88 43 35 56 36 97 16 48 92 35 41 30 63 46 68 23 74 42 79 08 94

.....  
.....  
.....

85 96 68 90 03 99 35 48 61 12 80 56 72 41 03 23 59 36 21 98 05 10 72

.....  
.....  
.....

70 40 96 47 58 47 26

.....  
.....  
.....

bericht 5:

44 99 69 35 68 85 44 88 35 80 90 03 47 86 31 90 26 99 31 56 47 57 54

.....  
.....  
.....

91 56 13 41 37 79 57 93 29 08 35 01 28 72 86 56 05 22 81 43 87 72 03

.....  
 .....  
 .....

52 85 86 78 10 03 99 87 12 36 91

.....  
 .....  
 .....

Codeertabel voor oplossing										
	1	2	3	4	5	6	7	8	9	0
1										
2										
3										
4										
5										
6										
7										
8										
9										
0										