

# 8 WERKBLAD SLEUTELS

## Inleiding

We kunnen een complexere manier van transpositieversleuteling bereiken door gebruik te maken van sleutelwoorden. Als voorbeeld nemen we de sleutel *"baldadig"*.

De letters van deze sleutel geven we nu een volgnummer, op volgorde van het alfabet. Je nummert van links naar rechts, dus als een letter meer dan één keer voorkomt zoals de *a*, dan nummer je zoals in Figuur 1A.

Van de volgende drie letters van het alfabet komt de *b* 1x voor, de *c* 0x en de *d* weer 2x: tel weer van links naar rechts (Figuur 1B). Op volgorde van het alfabet komen we dan uiteindelijk tot het eindresultaat in Figuur 1C.

Dit resultaat gebruiken we om de klare tekst "ik maak me grote zorgen over de geheimen" te versleutelen. In Figuur 2D is de klare tekst in rijen onder de sleutel geschreven, zodat er kolommen met letters ontstaan onder de sleutel.

Vervolgens zijn deze kolommen in Figuur 2E als rijen opgeschreven (een kwartslag gedraaid, dus) op volgorde van de nummering van de sleutel (Figuur 1C), dus de kolom a1 staat bovenaan.

Door de rijen in Figuur 2E van boven naar beneden achter elkaar op te schrijven ontstaat de uiteindelijke cijfertekst:

"KREEAEVIIGGGATOEKZEMERENMODEMONH".

## Opdracht A

Op de volgende bladzijde vind je een invulschema. Voer daar de volgende opdrachten uit:

1. Gebruik de sleutel *"babytaal"* om de klare tekst "het wapen is begraven bij de schommels" te versleutelen.
2. Beredeneer of het mogelijk is om met een andere sleutel tot dezelfde cijfertekst te komen.

## Opdracht B

Om een cijfertekst die met dit algoritme versleuteld is weer te ontcijferen, moet het schema in omgekeerde volgorde worden uitgevoerd. Je ontvangt de cijfertekst:

"ESLVVGOARTVDVANIAEOGEADJOTARDLPR".

Met de verzender heb je de sleutel *"zaterdag"* afgesproken.

3. Ontcijfer dit bericht.

## Opdracht C

4. Versleutel een zelfbedachte klare tekst met een zelfbedachte sleutel. Geef de cijfertekst en de sleutel aan een klasgenoot en laat deze jouw cijfertekst ontcijferen.

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| A | b | a | l | d | a | d | i | g |
|   |   | 1 |   |   | 2 |   |   |   |
| B | b | a | l | d | a | d | i | g |
|   | 3 | 1 |   | 4 | 2 | 5 |   |   |
| C | b | a | l | d | a | d | i | g |
|   | 3 | 1 | 8 | 4 | 2 | 5 | 7 | 6 |

FIGUUR 1

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| D | b | a | l | d | a | d | i | g |
|   | 3 | 1 | 8 | 4 | 2 | 5 | 7 | 6 |
| E | i | k | m | a | a | k | m | e |
|   | g | r | o | t | e | z | o | r |
|   | g | e | n | o | v | e | d | e |
|   | g | e | h | e | i | m | e | n |
|   |   |   |   |   |   |   |   |   |
|   | a | 1 |   |   |   |   |   |   |
|   | a | 2 |   |   |   |   |   |   |
|   | b | 3 |   |   |   |   |   |   |
|   | d | 4 |   |   |   |   |   |   |
|   | d | 5 |   |   |   |   |   |   |
|   | g | 6 |   |   |   |   |   |   |
|   | i | 7 |   |   |   |   |   |   |
|   | l | 8 |   |   |   |   |   |   |
|   |   |   | k | r | e | e |   |   |
|   |   |   | a | e | v | i |   |   |
|   |   |   | i | g | g | g |   |   |
|   |   |   | a | t | o | e |   |   |
|   |   |   | k | z | e | m |   |   |
|   |   |   | e | r | e | n |   |   |
|   |   |   | m | o | d | e |   |   |
|   |   |   | m | o | n | h |   |   |

FIGUUR 2

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| z | a | t | e | r | d | a | g |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |

[illegible][illegible]

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| b | a | b | y | t | a | a | l |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |

|  |   |
|--|---|
|  | 1 |
|  | 2 |
|  | 3 |
|  | 4 |
|  | 5 |
|  | 6 |
|  | 7 |
|  | 8 |

[illegible]

|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |   |
|--|---|
|  | 1 |
|  | 2 |
|  | 3 |
|  | 4 |
|  | 5 |
|  | 6 |
|  | 7 |
|  | 8 |

[illegible]