**Antwoorden les 2: Affiene versleuteling**

**Opgave 1**
a. 133 - 5 ·26 = 3, dus "D".
b. Verschillen 26.
c.2662 - 2652 = 10, dus "K".
d. -22 + 26 = 4, dus "E".

**Opgave 2**a. *E*7(*x*) = *x* + 7
*b. E*-9(*x*) = *x-*9
*c. Ek*(*x*) = *x* + *k*

**Opgave 3***a. D*3(*x*) = *x* - 3
b.*Dk*(*x*) = *x* - *k*

**Opgave 4**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Klare tekst | a  | b  | c  | d  | e  | f  | g  | h  | i  | j  | k  | l  | m |
| code  | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10  | 11  | 12  |
| *E*11(*x*)=REST((*x*+11):26 | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| *E*(5,6)(*x*)=REST((5*x*+6):26) | G | L | Q | V | A | F | K | P | U | Z | E | J | O |
| *E*(9,2)(*x*)=REST((9*x*+2):26) | C | L | U | D | M | V | E | N | W | F | O | X | G |
| *E*(3,8)(*x*)=REST((3*x*+8):26) | I | L | O | R | U | X | A | D | G | P | M | J | X |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Klare tekst | n | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| code | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| *E*11(*x*)=REST((*x*+11):26 | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| *E*(5,6)(*x*)=REST((5*x*+6):26) | T | Y | D | I | N | S | X | C | H | M | R | W | B |
| *E*(9,2)(*x*)=REST((9*x*+2):26) | P | Y | H | Q | Z | I | R | A | J | S | B | K | T |
| *E*(3,8)(*x*)=REST((3*x*+8):26) | V | Y | B | E | H | K | N | Q | T | W | Z | C | F |

**Opgave 5**
a. Hgtgh ytvYO XUATC CNKGG XPAXK ALACN ATRWB
b. Ik zal er zijn en draag een geel kanariepak.

**Opgave 6**Dan worden alle letters vercijferd als de letter *d*.

**Opgave 7**
*a*=1 en *b*=*k*

**Opgave 8**
a. JDLFB en JDLFB.
b. DHLPTXBFJNRVZ DHLPTXBFJNRVZ
c. Je krijgt slechts de helft van de letters terug in het vercijferde alfabet.
d. De functie *y* = 4*x*+3 heeft alleen oneven uitkomsten, ook als je er een veelvoud van 26 aftrekt. Hierdoor kun je niet op alle posities terecht komen.

**Opgave 9**
a. Je krijgt of alle oneven of alle even getallen < 26, maar nooit alle getallen < 26.
b. Je krijgt alleen even uitkomsten, nee dus.
c. Als we achtereenvolgens 0, 1, 2, 3, ... invullen, krijgen we er 0, 3, 6, 9, 12, 15, 18, 21, 24, 1, 4, 7, 10, 13, 16, 19, 22, 25, 2, 5, 8, 11, 14, 17, 20, 23 uit, dus eerst de drievouden, dan de drievouden +1 en dan de drievouden +2. Dus alle getallen van 0 t/m 25.
d. Nee, je krijgt er alleen 0 en 13 uit.
e. Voor *a =*1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. (Dus voor alle oneven getallen behalve 13.)
f. *E*(*a*+26,*b*)(*x*) = rest((*x*·(*a*+26)+*b*):26 = rest((*ax*+26*x*+b):26) = rest((*ax*+b):26) = *E*(*a*,*b*)(*x*)
 **Opgave 10**
a. 25, bij *m*=0 is de cijfertekst identiek aan de klare tekst.
b. In opgave 7 zagen we dat er voor *a*12 mogelijke getallen zijn, *b*kan gekozen worden uit de getallen 0 t/m 25. Vercijfering met *a* = 1 en *b* = 0 levert de klare tekst en heeft dus geen zin. Er zijn dus 12·26 - 1 = 311 sleutelparen. Vercijfering met *a* = 0 en een willekeurige *b* levert altijd *b* op als vercijfering. Deze vercijferingen zijn dus ook zinloos. Aldus komen we op 311 - 26 = 285 sleutelparen.

**Opgave 11**a. Uit *E*(*a*,*b*)(3) = 16 volgt dat er een *a* en een *b* moeten zijn waarvoor geldt
rest(*a*·3 + *b*):26 = 16. Dit betekent dat (*a*·3 + *b*) = 16 +*p*·26
b. *E*(*a*,*b*)(13) = 14 betekent dat (*a*·3 + *b*) = 14 +*q*·26
c. Als de beweringen bij onderdeel a) en b) beide moeten gelden dan levert dit het genoemde stelsel op.
d. Voor het sleutelpaar geldt: (*a,b*) = (5,1). Berekening:



e. Uit *E*(18,14)(*x*) = 18*x* + 14 volgt dat de cijfercode altijd even is. Dit levert de helft van de letters van het alfabet en allemaal 2x.

**Opgave 12**
a. c = 2, f = 5, e = 4
De sleutel is (17, 23). Berekening:

 Dit volgt direct uit de kraak-tabel

b. d = 3, N = 12. h = 7 J = 9
De sleutel is (12 , 3 ). Dit volgt direct uit de kraak-tabel.