# Universiteit van Stellenbosch

## Toegepaste Wiskunde 314

### Tutoriaal 2: Donderdag 26 Februarie 2004

**MEMORANDUM**

(1)  (a)  $\phi(1\,024) = \phi(2^{10}) = 512$

  (b)  $\phi(541) = 540$ (541 is priem)

  (c)  $\phi(54\,054) = \phi(2 \times 3^3 \times 7 \times 11 \times 13) = 12\,960$

(2)  (a)  $\phi(24) = \phi(2^3 \times 3) = 8$

  (b)  $\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$

  (c)

| $\times$ | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
| 5 | 5 | 1 | 11 | 7 | 17 | 13 | 23 | 19 |
| 7 | 7 | 11 | 1 | 5 | 19 | 23 | 13 | 17 |
| 11 | 11 | 7 | 5 | 1 | 23 | 19 | 17 | 13 |
| 13 | 13 | 17 | 19 | 23 | 1 | 5 | 7 | 11 |
| 17 | 17 | 13 | 23 | 19 | 5 | 1 | 11 | 7 |
| 19 | 19 | 23 | 13 | 17 | 7 | 11 | 1 | 5 |
| 23 | 23 | 19 | 17 | 13 | 11 | 7 | 5 | 1 |

(3)  (a)  $x \equiv 8 \pmod{28}$

  (b)  Geen oplossings

  (c)  $x \equiv 6, 13, 20, 27 \pmod{28}$

(4)  $(x, y) \equiv (2, 12) \pmod{26}$ of $(x, y) \equiv (15, 12) \pmod{26}$.

(5)  $90 \times \phi(90) = 90 \times \phi(2 \times 3^2 \times 5) = 90 \times 24 = 2\,160$

(6)  Kriptoteks: `OERJEFV`

(7)  Skoonteks: `wielderoftheflameofarnor`, oftewel "wielder of the flame of Arnor"

(8)  (a)  'n Brute–krag soektog, soos in Voorbeeld 2-8 op bladsy 37 van die klasnotas, lewer die sleutel $(a, b) = (17, 5)$, en die skoonteks is

  `atalmostthesametimeasgandalfhadarrivedinmiddleearthadarkpowerhada`
  `ppearedinsouthernmirkwoodattheevilplaceknownasdolguldurafterathou`
  `sandyearsofhiswanderingsgandalfwentthereanddrovethedarknessintoth`
  `eeastforawhilesoonitreturnedandintheyeartwothousandfourhundredand`
  `sixtythreeofthethirdagethegreatestamongwizardsandelvesformedawhit`
  `ecouncilwithgandalfasaprominentmembertocounterthegrowingthreatint`
  `wothousandeighthundredandfiftygandalfrevisiteddolguldurtofindthat`
  `thepowerthatheldithadgrownindeedduringtheeighthundredyearssincehi`

```
slastvisiteerecognisedthedarkpowernowassauronreturnedandescapedto
informthewhitecouncilbeforeheescapedthoughhefoundthrainiibrokenin
thepitsofdolguldurandthoughthraindiedbeforegandalfcouldhelphimhed
idsurrenderamapandakeyintothewizardskeeping
```

oftewel

"At almost the same time as Gandalf had arrived in middle earth a dark power had appeared in southern Mirkwood at the evil place known as Dol Guldur. After a thousand years of his wanderings Gandalf went there and drove the darkness into the east for a while. Soon it returned and in the year two thousand four hundred and sixty three of the third age the greatest among wizards and elves formed a White Council with Gandalf as a prominent member to counter the growing threat. In two thousand eight hundred and fifty gandalf revisited Dol Guldur to find that the power that held it had grown indeed during the eight hundred years since his last visit. He recognised the dark power now as Sauron returned and escaped to inform the White Council. Before he escaped, though, he found Thrain II broken in the pits of Dol Guldur and though Thrain died before Gandalf could help him he did surrender a map and a key into the wizard's keeping."

(na invoeging van spasies en leestekens)

(b) Die volgende letterfrekwensies word in die kriptoteks waargeneem:

| | | | | | |
|---|---|---|---|---|---|
| A: | 13 | J: | 48 | S: | 58 |
| B: | 13 | K: | 23 | T: | 8 |
| C: | 0 | L: | 51 | U: | 51 |
| D: | 22 | M: | 19 | V: | 92 |
| E: | 63 | N: | 11 | W: | 4 |
| F: | 68 | O: | 2 | X: | 6 |
| G: | 1 | P: | 18 | Y: | 6 |
| H: | 26 | Q: | 65 | Z: | 34 |
| I: | 56 | R: | 0 | | |

Hierdie frekwensies suggereer dat e enkripteer na V en dat t enkripteer na F, wat impliseer dat die sleutelpaar die kongruensies

$$\begin{cases} 4a + b &\equiv 21 \ (\text{mod } 26) \\ 19a + b &\equiv 5 \ (\text{mod } 26) \end{cases}$$

bevredig, wat as oplossing die unieke sleutelpaar $(a, b) = (18, 1)$ het. Hierdie sleutelpaar is egter nie korrek nie, aangesien die kriptoteks na dekripteer na verstaanbare Engelse teks as die paar gebruik word nie. As tweede raaiskoot vermoed ons dus dat e enkripteer na V en dat t enkripteer na Q, wat impliseer dat die sleutelpaar die kongruensies

$$\begin{cases} 4a + b &\equiv 21 \ (\text{mod } 26) \\ 19a + b &\equiv 16 \ (\text{mod } 26) \end{cases}$$

bevredig, wat as oplossing die unieke sleutelpaar $(a, b) = (17, 5)$ het. Hierdie sleutelpaar is korrek, soos ook in (a) gevind.