Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 2: Donderdag 26 Februarie 2004

(1) Vind die volgende waardes vir die bekende Euler–funksie:

(a) $\phi(1\,024)$

(b) $\phi(541)$

(c) $\phi(54\,054)$

(2) (a) Bepaal $\phi(24)$.

(b) Gebruik die Gewysigde Euklidiese Algoritme om die versameling $\mathbb{Z}_{24}^*$ te bepaal.

(c) Bevestig dat $(\mathbb{Z}_{24}^*, \times)$ 'n groep is (waar '$\times$' vermenigvuldiging modulo 24 aandui), deur 'n vermenigvuldigingstabel vir $\mathbb{Z}_{24}^*$ op te stel.

(3) Vind in elk van die onderstaande gevalle alle oplossings $x \in \mathbb{Z}_{28}$ van die gegewe lineêre kongruensie:

(a) $3x \equiv 24 \pmod{28}$

(b) $4x \equiv 25 \pmod{28}$

(c) $4x \equiv 24 \pmod{28}$

(4) Vind alle oplossings $(x, y) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ van die sisteem van lineêre kongruensies:

$$\begin{cases} 2x + y & \equiv & 16 \pmod{26} \\ 2x - y & \equiv & 18 \pmod{26} \end{cases}$$

(5) Wat is die grootte van die affiene substitusie stelsel, as 'n alfabet wat uit 90 karakters bestaan, gebruik word?

(6) Enkripteer, *met die hand*, die skoonteks `gandalf` volgens die affiene substitusie stelsel $\aleph_{26}^{19,4}$. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Block ciphers", en daarna op "Affine substitution".]

(7) Dekripteer, *met die hand*, die skoonteks `RTBAQBOHMKIBMAJLBHMJOWHO` volgens die affiene substitusie stelsel $\aleph_{26}^{11,9}$. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Block ciphers", en daarna op "Affine substitution".]

(8) Die kriptoteks

```
FQFKBJZQQUVZFBVQLBVFZDFSEFKMUFEFIILYVELSBLEEKVVFIQUFEFITAJPVIUFEFAA
VFIVELSZJHQUVISBLITPJJEFQQUVVYLKAKFNVTSJPSFZEJKDHKEHIFMQVIFQUJHZFSE
XVFIZJMULZPFSEVILSDZDFSEFKMPVSQQUVIVFSEEIJYVQUVEFITSVZZLSQJQUVVFZQM
```

```
JIFPULKVZJJSLQIVQHISVEFSELSQUVXVFIQPJQUJHZFSEMJHIUHSEIVEFSEZLGQXQUI
VVJMQUVQULIEFDVQUVDIVFQVZQFBJSDPLOFIEZFSEVKYVZMJIBVEFPULQVNJHSNLKPL
QUDFSEFKMFZFAIJBLSVSQBVBWVIQJNJHSQVIQUVDIJPLSDQUIVFQLSQPJQUJHZFSEVL
DUQUHSEIVEFSEMLMQXDFSEFKMIVYLZLQVEEJKDHKEHIQJMLSEQUFQQUVAJPVIQUFQUV
KELQUFEDIJPSLSEVVEEHILSDQUVVLDUQUHSEIVEXVFIZZLSNVULZKFZQYLZLQVVIVNJ
DSLZVEQUVEFITAJPVISJPFZZFHIJSIVQHISVEFSEVZNFAVEQJLSMJIBQUVPULQVNJHS
NLKWVMJIVUVVZNFAVEQUJHDUUVMJHSEQUIFLSLLWIJTVSLSQUVALQZJMEJKDHKEHIFS
EQUJHDUQUIFLSELVEWVMJIVDFSEFKMNJHKEUVKAULBUVELEZHIIVSEVIFBFAFSEFTVX
LSQJQUVPLOFIEZTVVALSD
```

is deur middel van die affiene substitusie stelsel $\aleph_{26}^{a,b}$ gevorm.

(a) Gebruik die program **EnDeCrypt** om 'n brutekrag soektog na die sleutelpaar $(a, b) \in \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$ te loots en sodoende die onderliggende skoonteks te ontrafel.

(b) Herhaal (a), maar gebruik hierdie keer 'n meer intelligente letterfrekwensie metode. [Wenk: U kan aanvaar die onderliggende skoonteks is Engelse prosa. Klik op "Crypto analysis" op die **EnDeCrypt** hoofspyskaart, daarna op "Letter frequencies" om letterfrekwensies in die begenoemde kriptoteks te bepaal.]

Ster Kinekor Uitdaging: Ontrafel die identiteit van die twee Griekse gode wat in die kriptoteks

APLF **CL** LWXAAX,

met mekaar kommunikeer, en verduidelik die meganisme agter die enkripsie. [Wenk: Die affiene substitusie speel 'n sterk rol in die bogenoemde kriptogram, alhoewel die gode nooit 'n (enkele) toepassing van die affiene substitusie gebruik het nie ...]