Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 1: Donderdag 19 Februarie 2004

(1) Vind in elk van die onderstaande gevalle die m–modulêre ekwivalensie klas van die gegewe getal:

(a) 14 ($m = 26$)

(b) 34 ($m = 16$)

(c) –29 ($m = 16$)

(d) 20 772 ($m = 26$)

(e) –77 484 ($m = 17$)

(2) Bewys Stelling 2–1(l) op bladsy 18 van die klasnotas.

(3) Enkripteer, *met die hand*, die skoonteks `romanempire` volgens die additiewe substitusie stelsel $\Im_{26}^{15}$. 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 "Additive substitution".]

(4) Dekripteer, *met die hand*, die kriptoteks `MXOLXV` wat met behulp van die Caesar–stelsel gevorm is. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**.

(5) Die kriptoteks `UKNMNL` is deur middel van die additiewe substitusie stelsel $\Im_{26}^{19}$ gevorm. Dekripteer die kriptoteks *met die hand*. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**.

(6) Die kriptoteks `PJVJHIJH` is deur middel van die additiewe substitusie stelsel $\Im_{26}^{s}$ gevorm. Gebruik die program **EnDeCrypt** om 'n brutekrag soektog na die sleutel s te loots en sodoende die onderliggende skoonteks te ontrafel.

(7) Gebruik die Euklidiese Algoritme om die grootste gemene delers van die volgende pare getalle *met die hand* te bereken:

(a) 264, 3 699

(b) 1 862, 2 090.

Gebruik die *Modular Calculator* van **EnDeCrypt** om die korrektheid van jou antwoord te toets. [Wenk: Klik op "Tools" op die **EnDeCrypt** hoofspyskaart, en daarna op "Modular Calculator". Gebruik die "GCD[ ]" knoppie, maar verseker dat die modulus groter as die grootste getal in die paar is waarvan die grootste gemene deler gevind moet word.]

(8) Gebruik die Gewysigde Euklidiese Algoritme om die multiplikatiewe inverses van die volgende getalle *met die hand* te bereken:

(a) 5 (mod 24)

(b) 5 (mod 14)

(c) 14 (mod 24).

Gebruik die *Modular Calculator* van **EnDeCrypt** om die korrektheid van jou antwoord te toets. [Wenk: Wenk: Klik op "Tools" op die **EnDeCrypt** hoofspyskaart, en daarna op "Modular Calculator". Gebruik dan magsverheffing ("^") met eksponent "(-1)", nadat jy die modulus gespesifiseer het. Klik op "=" om antwoorde te verkry.]

Marcel's Frozen Yoghurt Uitdaging: Ontrafel die betekenis van die kriptoteks

`DRQPAKYO`,

en verduidelik die meganisme agter die enkripsie.