Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 5: Donderdag 18 Maart 2004

(1) Skakel die getal 213 om na die binêre voorstelling daarvan.

(2) Skakel die getal $(11001001)_2$ om na die desimale voorstelling daarvan.

(3) (a) Bepaal die twee sub–sleutels van die vereenvoudigde DES stelsel uit die oorspronklike sleutel $\underline{k} = [1, 1, 1, 0, 0, 0, 1, 0, 1, 0]$.

(b) Enkripteer, *met die hand*, die skoonteks "£" volgens die vereenvoudigde DES stelsel, met sleutel $\underline{k} = [1, 1, 1, 0, 0, 0, 1, 0, 1, 0]$. 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 "Simplified DES".]

(c) Dekripteer, *met die hand*, die kriptoteks "°" volgens die vereenvoudigde DES stelsel, met sleutel $\underline{k} = [1, 1, 1, 0, 0, 0, 1, 0, 1, 0]$. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**.

(4) Probleme 1(a) en 1(b) op bladsy 128 van die klasnotas.

(5) Probleem 2 op bladsy 128 van die klasnotas.

(6) Probleem 3(a) op bladsy 128 van die klasnotas.

(7) Gebruik 'n muntstuk om 24 bisse ewekansig op te wek. Voldoen hierdie substroom aan die postulate van Golomb?

(8) Gebruik 'n Vernam–stelsel om die skoonteks `DES` met sleutel soos in vraag (7) *met die hand* te enkripteer. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**. [Wenk: Klik op "Crypto systems" op die **EnDeCrypt** hoofspyskaart, daarna op "Stream ciphers", en daarna op "Vernam".]

(9) Die kriptoteks

$$\underline{t} = \mathtt{1,1,1,0,1,0,0,0,0,1,1,0,1,0,0,1,1,1,1,0,0,1,0,0}$$

is deur middel van 'n Vernam stelsel met sleutelsubstroom

$$\underline{s} = \mathtt{1,0,1,1,1,0,1,0,0,0,1,1,1,0,1,0,1,0,1,0,0,1,0,1}$$

genereer. Wat is die ooreenstemmende skoonteks (i.t.v. ASCII–karakters)?