Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 5: Donderdag 18 Maart 2004

MEMORANDUM

(1) $213 \equiv (11010101)_2$.

(2) $(11001001)_2 \equiv 201$.

(3) (a) Om die subsleutel $\underline{s}^0$ uit die sleutel $\underline{k} = [1,1,1,0,0,0,1,0,1,0]$ te bereken, word $\underline{P}$ eers toegepas op $\underline{k}$ om $\underline{P}(\underline{k}) = [1,0,1,1,0,0,1,1,0,0]$ te vind. Daarna word elke bis in $\underline{P}(\underline{k})$ met $R_0 = 1$ posisie na links (modulo 10) geroteer om $(R_0 \circ \underline{P})(\underline{k}) = [0,1,1,0,0,1,1,0,0,1]$ te vorm. $\underline{s}^0$ word dan verkry deur die bisseleksie $\underline{Q}$ op $(R_0 \circ \underline{P})(\underline{k})$ toe te pas, en sodoende

$$\underline{s}^0 = (\underline{Q} \circ R_0 \circ \underline{P})(\underline{k}) = [1,1,1,0,0,0,1,0]$$

te verkry. Om $\underline{s}^1$ te bereken, word die Feistel–operator eers op $(R_0 \circ \underline{P})(\underline{k})$ teogepas om $(F \circ R_0 \circ \underline{P})(\underline{k}) = [1,1,0,0,1,0,1,1,0,0]$ te verkry. Daarna word elke bis in $(F \circ R_0 \circ \underline{P})(\underline{k})$ met $R_1 = 2$ posisies na links (modulo 10) geroteer, om $(R_1 \circ F \circ R_0 \circ \underline{P})(\underline{k}) = [0,0,1,0,1,1,0,0,1,1]$ te lewer. Die subsleutel $\underline{s}^1$ word dan verkry deur die bisseleksie $\underline{Q}$ op $(R_1 \circ F \circ R_0 \circ \underline{P})(\underline{k})$ toe te pas, waaruit volg dat

$$\underline{s}^1 = (\underline{Q} \circ R_1 \circ F \circ R_0 \circ \underline{P})(\underline{k}) = [1,1,0,0,0,1,1,1].$$

(b) Gestel nou die karakter "£" moet met behulp van die vereenvoudigde DES stelsel met subsleutels $\underline{s}^0 = [1,1,1,0,0,0,1,0]$ en $\underline{s}^1 = [1,1,0,0,0,1,1,1]$ geenkripteer word. Die karakter "£" het 'n ASCII–waarde van 156, wat binêr versyfer kan word as $\underline{x} = [1,0,0,1,1,1,0,0]$. Deur die permutasie $\underline{I}$ op $\underline{x}$ toe te pas, vind ons $\underline{I}(\underline{x}) = [0,1,0,1,1,0,1,0]$. Die funksie $\underline{T}_0$ opereer nou op die laaste 4 bisse van hierdie string, naamlik $\underline{n}^0 = [n_4^0, n_5^0, n_6^0, n_7^0] = [1,0,1,0]$. Vorm die modulo–diagram

$$\begin{array}{c|cc|cc} n_7^0 & n_4^0 & n_5^0 & n_6^0 & \\ n_5^0 & n_6^0 & n_7^0 & n_4^0 & \end{array} = \begin{array}{c|cc|c} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{array}$$

en tel hierdie inskrywings (modulo 2) by die $\underline{s}^0$ om

$$\begin{array}{c|ccc|c} u_0^0 = 0 \oplus 1 \equiv 1 & u_1^0 = 1 \oplus 1 \equiv 0 & u_2^0 = 0 \oplus 1 \equiv 1 & u_3^0 = 1 \oplus 0 \equiv 1 \\ v_0^0 = 0 \oplus 0 \equiv 0 & v_1^0 = 1 \oplus 0 \equiv 1 & v_2^0 = 0 \oplus 1 \equiv 1 & v_3^0 = 1 \oplus 0 \equiv 1 \end{array}$$

te verkry. Nou is $u_0^0 u_3^0 = 11$ en $u_1^0 u_2^0 = 01$, sodat, uit ry 3 en kolom 1 van $S[0]$, volg dat $w_0^0 w_1^0 = 01$, wat die binêre versyfering van 1 is. Soortgelyk is $v_0^0 v_3^0 = 01$ en $v_1^0 v_2^0 = 11$, sodat, uit ry 1 en kolom 3 van $S[1]$, volg dat $w_2^0 w_3^0 = 11$, wat die binêre versyfering van 3 is. Gevolglik is $\underline{T}_0(\underline{n}^0) = [1,1,1,0]$ en dus is

$$(\underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x}) = [0 \oplus 1, 1 \oplus 1, 0 \oplus 1, 1 \oplus 0, 1, 0, 1, 0] \equiv [1,0,1,1,1,0,1,0].$$

Deur die Feistel–operator op $(\underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x})$ toe te pas, vind ons $(F \circ \underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x}) = [1,0,1,0,1,0,1,1]$. Die funksie $\underline{T}_1$ opereer nou op die laaste 4 bisse van $(F \circ \underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x})$, naamlik $\underline{n}^1 = [n_4^1, n_5^1, n_6^1, n_7^1] = [1,0,1,1]$. Vorm die modulo–diagram

$$\begin{array}{c|cc|c} n_7^1 & n_4^1 & n_5^1 & n_6^1 \\ n_5^1 & n_6^1 & n_7^1 & n_4^1 \end{array} = \begin{array}{c|cc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{array}$$

en tel die inskrywings van die subsleutel $\underline{s}^1$ (modulo 2) by hierdie inskrywings om

$$\begin{array}{c|cc|c} u_0^1 = 1 \oplus 1 \equiv 0 & u_1^1 = 1 \oplus 1 \equiv 0 & u_2^1 = 0 \oplus 0 \equiv 0 & u_3^1 = 1 \oplus 0 \equiv 1 \\ v_0^1 = 0 \oplus 0 \equiv 0 & v_1^1 = 1 \oplus 1 \equiv 0 & v_2^1 = 1 \oplus 1 \equiv 0 & v_3^1 = 1 \oplus 1 \equiv 0 \end{array}$$

te verkry. Nou is $u_0^1 u_3^1 = 01$ en $u_1^1 u_2^1 = 00$, sodat, uit ry 1 en kolom 0 van $S[0]$, volg dat $w_0^1 w_1^1 = 11$, wat die binêre versydering van 3 is. Verder is $v_0^1 v_3^1 = 00$ en $v_1^1 v_2^1 = 00$, sodat, uit ry 0 en kolom 0 van $S[1]$, volg dat $w_2^1 w_3^1 = 00$, wat die binêre versyfering van 0 is. Gevolglik is $\underline{T}_1(\underline{n}^1) = [1,0,0,1]$ en dus is

$$(\underline{\Pi}_{\underline{T}_1} \circ F \circ \underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x}) = [1 \oplus 1, 0 \oplus 0, 1 \oplus 0, 0 \oplus 1, 1, 0, 1, 1] \equiv [0,0,1,1,1,0,1,1].$$

Uiteindelik verkry ons die binêre vorm van die kriptoteks deur die inverse permutasie $\underline{I}^{-1}$ op die bogenoemde resultaat toe te pas, en vind dat

$$\underline{y} = (\underline{I}^{-1} \circ \underline{\Pi}_{\underline{T}_1} \circ F \circ \underline{\Pi}_{\underline{T}_0} \circ \underline{I})(\underline{x}) = [1,0,1,1,1,0,1,0],$$

wat die binêre voorstelling van 186 is. Uit die ASCII–tabel volg dit dus dat die kriptotekskarakter "||" is.

(c) Gestel die karakter "°" moet met behulp van die vereenvoudigde DES stelsel met sleutel $\underline{k} = [1,1,0,0,1,0,1,0,1,1]$ gedekripteer word. Die karakter "°" het 'n ASCII–waarde van 167, wat binêr versyfer kan word as $\underline{y} = [1,0,1,0,0,1,1,1]$. Nou lewer die binêre transformasies

$$\underline{x} = (\underline{I}^{-1} \circ \underline{\Pi}_{\underline{T}_0} \circ F \circ \underline{\Pi}_{\underline{T}_1} \circ \underline{I})(\underline{y}) = [0,1,0,0,1,1,0,1],$$

op 'n soorgelyke manier as in vraag 3(b), wat die binêre voorstelling van 77 is. Uit die ASCII–tabel volg dit dus dat die kriptotekskarakter "M" is.

(4) (a) Postulaat 1 word nie bevredig nie (6 nulle & 12 ene); Postulaat 2 word nie bevredig nie (3 lopies van lengte 2 verwag, 0 teëgekom); Postulaat 3 word nie bevredig nie (auto–korrelasie funksie is 4–waardig).

(b) Al drie die postulate van Golomb word bevredig.

(5) Gebruik jou verbeelding ...

(6) $\underline{k}$ = `11101100 01010101 10100010`.

(7) Die antwoord hang af van die uitkomste van die 24 gooie van die muntstuk, maar dit is byna seker dat al drie die postulate van Golomb nie deur die stroom bevredig sal word nie.

(8) Die antwoord op hierdie vraag hang weereens af van die antwoord op vraag (7).

(9) Die skoonteks is `01010010 01010011 01000001`. Die desimale waardes van hierdie drie grepe is 82, 83 en 65. Die skoonteks verletter dus volgens die ASCII–tabel (Tabel 2-10 op bladsy 67 van die klasnotas) as `RSA`.