Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 4: Donderdag 11 Maart 2004

(1) Enkripteer, *met die hand*, die skoonteks `sirwinstonschurchill` volgens die kolom transposisie stelsel $\mathcal{C}_{26}^{5,\pi_1}$, met sleutel $\pi_1 = [3,1,2,5,4]$. 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 "Column transposition".]

(2) Dekripteer, *met die hand*, die kriptoteks `NIDEGSANNETECWENTAHIRPEPSTIOOINISMOS TIHEGPUNIHTWHCIWIIWHLONLPTUT` volgens die kolom transposisie stelsel $\mathcal{C}_{26}^{4,\pi_2}$, met sleutel $\pi_2 = [2,4,3,1]$. Toets die korrektheid van jou antwoord deur middel van die program **EnDeCrypt**.

(3) Die kriptoteks `ITHSRWOYLBILKNEITMDOFREOITINNTEDWIORETTI` is deur middel van die kolom transposisie stelsel $\mathcal{C}_{26}^{n,\pi_3}$ gevorm. Wat is die sleutel π_3 en die ooreenstemmende skoonteks?

(4) (a) Konstrueer 'n permutasie van lengte *groter* as 6 wat dieselfde enkripsie van enige skoonteks van lengte 24 karakters onder die kolom–transposisie stelsel sal lewer as met die sleutel $\pi = [1,3,2,4,6,5]$.

(b) Konstrueer 'n permutasie van lengte *kleiner* as 6 wat dieselfde enkripsie van enige skoonteks van lengte 24 karakters onder die kolom–transposisie stelsel sal lewer as met die sleutel $\pi = [1,3,2,4,6,5]$.

(5) Watter van die volgende matrikse is nie-singulier in die versameling $\mathcal{Z}_{26}^{n*}$? Motiveer.

(a) $\mathbf{S_1} = \begin{bmatrix} 4 & 17 \\ 7 & 13 \end{bmatrix}$ $(n=2)$

(b) $\mathbf{S_2} = \begin{bmatrix} 11 & 16 \\ 9 & 2 \end{bmatrix}$ $(n=2)$

(c) $\mathbf{S_3} = \begin{bmatrix} 11 & 16 & 5 \\ 9 & 2 & 14 \\ 19 & 19 & 8 \end{bmatrix}$ $(n=3)$

(d) $\mathbf{S_4} = \begin{bmatrix} 15 & 1 & 9 \\ 7 & 5 & 25 \\ 16 & 12 & 3 \end{bmatrix}$ $(n=3)$

(6) Bereken die inverses van die nie–singuliere matrikse in vraag 5.

(7) (a) Enkripteer, *met die hand*, die skoonteks `ipromisebloodtearstoilandsweat` volgens die Hill stelsel $\mathcal{H}_{26}^{2,\mathbf{S}_1}$. 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 "Hill transposition".]

(b) Herhaal vraag 6(a), maar gebruik hierdie keer die Hill stelsel $\mathcal{H}_{26}^{3,\mathbf{S}_3}$.

(8) (a) Dekripteer, deur middel van die program **EnDeCrypt**, die kriptoteks `BTDRYGR DWGPHUETHYEYOLIOEIUDNTHYEJBCEUNKNVHWGXHSDDNYCWAYQCCOF` volgens die Hill transposisie stelsel $\mathcal{H}_{26}^{2,\mathbf{S}_1}$.

(b) Dekripteer, deur middel van die program **EnDeCrypt**, die kriptoteks `RKMTSNT MIZHUEGMTCZDRINKJIGOIDTCAIFAXWPBRREQOIWYBFCKUGAWIOZAM` volgens die Hill transposisie stelsel $\mathcal{H}_{26}^{3,\mathbf{S}_3}$.

(9) Gebruik die inligting dat `oldstatesman` onder die Hill stelsel $\mathcal{H}_{26}^{n,\mathbf{S}_5}$ na `XZECPFILOXWV` enkripteer, om 'n (skoonteks, kriptoteks)–paar aanval op die sisteem te loots en sodoende die betekenis van die kriptoteks `IDAUPQDJTSPD` te ontrafel.

(10) Skryf neer die 5×5 Hill sleutel, $\mathbf{S}^{\pi_1}$, wat ooreenstem met die kolom transposisie sleutel π_1 in vraag 1. Enkripteer weer die skoonteks `sirwinstonschurchill`, maar gebruik hierdie keer die Hill stelsel $\mathcal{H}_{26}^{5,\mathbf{S}^{\pi_1}}$, en toets dat jy dieselfde antwoord as in vraag 1 verkry.

Debonairs Uitdaging: Ontrafel die betekenis van die kriptoteks

`UKJXRSMEGSQSISWFODXQLKRSEEPJGPRGRSVVDLOTIPXWWHRYGVJBYPAZGWBD`

wat met behulp van die Hill stelsel $\mathcal{H}_{26}^{n,\mathbf{S}_6}$ gevorm is.