Szyfr Hilla

7 stycznia 2014

Szyfrowania

Kluczem jest macierz np. $K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$, tekst do zaszyfrowania (np. july) przedstawiamy w postaci par liczb (ju-[9,20], ly-[11,24]). Szyfrowanie odbywa się poprzez pomnożenie liczb odpowiadającym tekstowi z kluczem: $[9, 20] \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = [99{+}60, 72{+}140] = [3, 4]$ (działanie modulo 26) oraz $[11, 24] \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix} = [121 + 72, 88 + 168] = [11, 22]$. Otrzymanym szyfrem jest tekst delw. Do odszyfrowania potrzebna jest macierz odwrotna do K. Jeżeli wyznacznik macierzy K jest odwracalny NWD(det K,26)=1, det K $= \begin{vmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{vmatrix} = k_{11}k_{22} - k_{12}k_{21}$ to macierz odwrotna do K dana jest wzorem $K^{-1} = (\det K)^{-1} \begin{bmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{bmatrix}$. Ogólnie $K^{-1} = (\det K)^{-1} K*$ gdzie K* to macierz, która na miejscu ij ma element o wartości $(-1)^{i+j} \det K_{ij}$. K_{ij} to macierz otrzymana z K bez i-tego wiersza i j-tej kolumny. W tym przykładzie $\det K = 1$, $K^{-1} = \begin{bmatrix} 7 & -8 \\ -3 & 11 \end{bmatrix} = \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$, deszyfrowanie $[3, 4] \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix} = [9, 20]$.

Atak ze znanym tekstem jawnym. Załóżmy, że szyfrowanie tekstu jawnego friday daje wynik pqcfku. Możemy zapisać, że [5,17]K=[15,16],[8,3]K=[2,5] i [0,24]K=[10,20]. Korzystając z pierwszych dwóch równań: $\begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix} K = \begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix}$. Należy teraz obliczyć $\begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix}^{-1}$ co daje $\begin{bmatrix} 5 & 17 \\ 8 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 9 & 1 \\ 2 & 15 \end{bmatrix}$ dzięki temu K $= \begin{bmatrix} 9 & 1 \\ 2 & 15 \end{bmatrix} \begin{bmatrix} 15 & 16 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 7 & 19 \\ 8 & 3 \end{bmatrix}$. Poprawność obliczeń można sprawdzić na trzeciej parze tekstu.

Zadanie: napisać program realizujący szyfr Hilla oraz dla podanego klucza przeprowadzić atak z tekstem jawnym.