

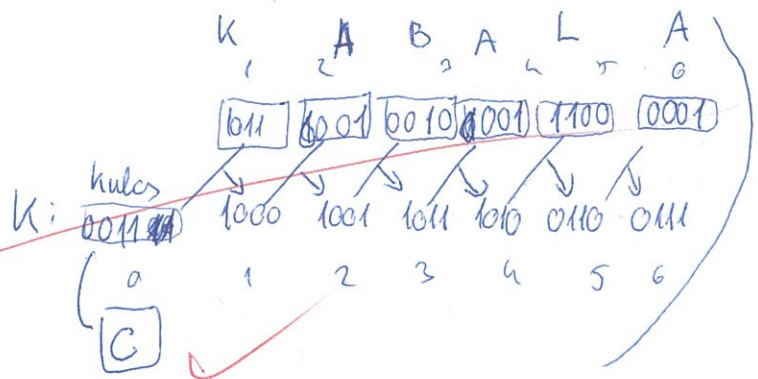
4 feladat: Titkosítás

SZÓ: K A B A L A

KÓD: H I K J F G

KULCS

művelet: vagy



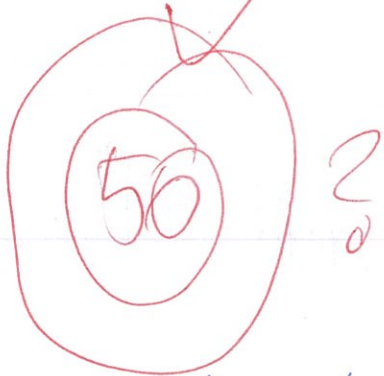
Az algoritmus a következő: A szó betűin/elemein az elejtől a végéig halad végig, a szó adott indexű, és az előző betűből fordított KÓD  $[i-1]$ -ből pedig a művelet segítségével számolja ki a következő betűt.

A művelet működése során a bemenetek bitjein egyszerre a VAGY/OR műveletet végzi el, tehát az eredményből és az egyik bemenetből egyértelműen meghatározható a bemenet.

\*másh

Igy a KÓD sorozatos elemeiből következtethetünk a nagyobb sorozatú elemmel párhuzamosan elhelyezkedő elemre a SZÓ-ban.

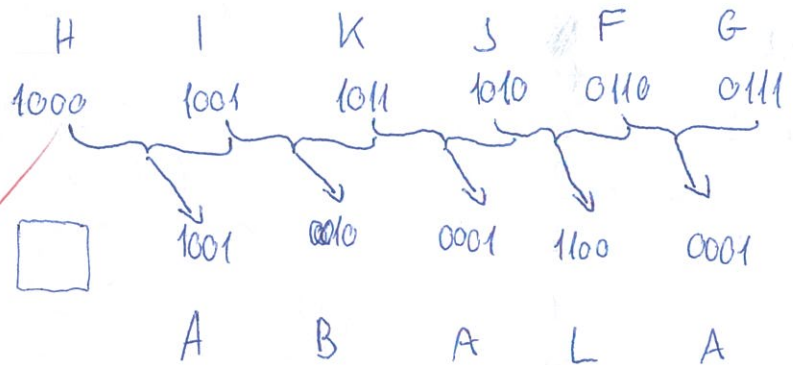
a kapott KÓD a betűket átírva:



elöl a szó 2-5.

betűinek kódjai

54?



A használható betűk közül az első betű helyére behelyettesítve csak a K-val kapunk értelmes magya szót

→ SZÓ: kabala

A K kódjából (1011) és a KÓD első eleméből (1000) pedig visszakövetkeztethető a KULCS:

"K" 1 0 1 1  
KULCS 0 0 1 1  
KÓD[1] 1 0 0 0

→ A KULCS a "C" (0011)

