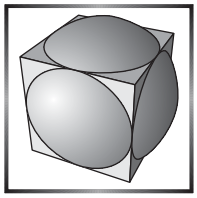
Az A pontversenyben kitűzött nehezebb feladatok (809–811.)



A. 809. Az ABC háromszög oldalai a szokásos jelölésekkel a, b és c, a súlypontja pedig S. Igazoljuk, hogy a háromszög síkjának tetszőleges P pontjára teljesül, hogy

$$a \cdot PA^3 + b \cdot PB^3 + c \cdot PC^3 \geqslant 3abc \cdot PS.$$

Javasolta: *Shultz János* (Szeged)

A. 810. Legyen minden pozitív egész n-re

$$r_n = \sum_{t=0}^{n} (-1)^t \binom{n}{t} \frac{1}{(t+1)!}.$$

Bizonyítsuk be, hogy $\sum\limits_{n=1}^{\infty} r_n = 0$.

A. 811. Adott egy n elemű A halmaz és egy $k < n$ pozitív egész szám. Határozzuk meg m legnagyobb lehetséges értékét, ha $i = 1, 2, \ldots, m$ esetén kiválaszthatók B_i és C_i halmazok úgy, hogy a következők teljesüljenek:

(*i*) $B_i \subset A$, $|B_i| = k$,

(*ii*) $C_i \subset B_i$ (C_i elemszámára nincs további megkötés),

(*iii*) minden $i \neq j$ esetén $B_i \cap C_j \neq B_j \cap C_i$.

❄

Beküldési határidő: 2021. december 10.
Elektronikus munkafüzet: `https://www.komal.hu/munkafuzet`

❄

„Titkos üzenet száll a széllel” II.*

Az első rész összefoglalása

A cikk első részében betekintettünk a titkosítás egyszerű módjaiba, majd megismertük a Napóleon használta Vigenère-kódolás mikéntjét és technikáját. Azt is megállapítottuk, hogy a monoalfabetikus kódolással szemben a nyelvi rendszer adta további szabályszerűség, a betűgyakoriságból adódó könnyű megfejtéstől is sikerült megszabadítanunk a titkos szöveget.

Ezt a titkosítási módszert feltörhetetlennek tartották és el is nevezték feltörhetetlen kódolásnak. De ez a vélekedés nem sokáig tartott, néhány évtizeddel Napóleon halála után, 1864-ben meg is született a megfejtés. Ugyan a folyamatos háborúskodás miatt nem hozták nyilvánosságra. Csak az első megoldó halála után, hagyatékának átvizsgálásakor derült ki az, hogy rájött a megoldásra, és az is, hogy milyen gondolatmenetet követett. Persze nem akárkiknek szokták tudományos alapossággal átvizsgálni a hagyatékát, az illető nem volt más, mint matematikus, kriptográfus, az informatika, a számítógéptudomány egyik korai nagy képviselője, a differenciálgép és az analitikai gép kitalálója, *Charles Babbage*.

A Vigenère-kódolás hiányossága

Vegyük végig Babbage gondolatmenetét. Ha valaki kellően eltökélt és veszi magának a fáradságot, nem szükséges semmiféle zsenialitás a kód megfejtéséhez. A módszer zsenialitását az adja, hogy az apró lépésekből Babbage olyan gondolatmenetet épített fel, amely elvezet a megfejtéshez akkor is, ha nem áll rendelkezésünkre a titkosítás kulcsa.

A kitalálói úgy vélték, hogy a Vigenère-kódolás megszabadít a nyelvi rendszertől, a betűgyakoriság elemzése nem vezet eredményre. Ez utóbbi igaz is, de a nyelvi rendszernek vannak még ennél is mélyebb megnyilvánulásai. Minden nyelvben vannak gyakorta előforduló betűhármasok, például az angol the, a német der, die, das, sch vagy a magyarban az egy. (Az olvasóra bízom, összeszámolja-e hány olyan magyar szót tud összegyűjteni, amelyben az egy, kov, kor jelsorozat szerepel, és hány olyat, amiben például a vöm vagy az űté.)

A további gondolatmenet könnyebb megértéséhez válasszunk egy rövid, négy jelből álló kulcsot. Legyen ez a BUSA. Vizsgáljuk meg, mivé kódolódhat az EGY jelsorozat. Ez persze attól függ, hogyan helyezkedik el az EGY jelsorozat a kulcshoz képest. Az E betű felett lehet B, U, S és végül A.

Titkosítsuk mind a négy esetet az előző részben megismert módszerrel.

kulcs:	B	U	S	A	B	U	S	A	B	U	S	A	B	U	S	A	B	U	S	A
nyers:	E	G	Y			E	G	Y			E	G	Y			E	G	Y		
titkos:	G	A	R			X	Y	Z			V	H	Á			É	Í	T		

Tehát az eredeti EGY négy különböző alakban jelenhet meg a titkos üzenetben: GAR, XYZ, VHÁ vagy ÉÍT. Ha elég hosszú a szöveg, várhatóan mind a négy többször előfordul majd. Látszólag egy fikarcnyival sem jutottunk közelebb a megoldáshoz, de csak látszólag.

A megfejtéshez vezető úton most nem kevés babramunka jön, ezt persze a mai gépek pillanatok alatt el tudnák végezni. Meg kell keresni a többször ismétlődő betűhármasokat és fel kell jegyezni az azonosak kezdőbetűinek távolságát. Használjuk továbbra is a fenti paramétereket. Tegyük fel, hogy a következő eredményt kaptuk:

betűhármasok	GAR (7db)	XYZ (3 db)	VHÁ (4 db)	ÉÍT(6 db)	...
a távolságuk az előző találattól:	36, 51, 11, 44, 120, 68	24, 36	12, 23, 27	16, 20, 32, 168, 48	...

Ha megvizsgáljuk, az egymás utáni távolságokra adódó számértékeket, azt találjuk, hogy néhány kivételtől eltekintve a számoknak van egy közös osztójuk. Húzzuk ki a sorból kilógókat:

$$36,\ \cancel{51},\ \cancel{11},\ 44,\ 120,\ 68,\ 24,\ 36,\ 12,\ \cancel{23},\ \cancel{27},\ 16,\ 20,\ 32,\ 168,\ 48.$$

Ezt már csak ügyesen értelmeznünk kell, továbbá magyarázatot találni a kilógó esetekre, és máris közelebb kerülünk a megoldáshoz. A valóságban ennél jóval több betűhármas fog ismétlődni, de nekünk most ennyi is elég. Az eltéréseknek nyilván az az oka, hogy azoknál az előfordulásoknál nem az EGY kódolódott GAR, XYZ, VHÁ vagy ÉÍT jelekké, mert azok más szórészletből is kialakulhatnak. Például:

kulcs:	B	U	S	A	B	U	S	A	B	U	S	A	B	U	S	A	B	U	S	A
titkos:			G	A	R	...										V	H	Á		
nyers:	...		Ó	Z	Ő	...										Ű	É	H		

Ami lehet értelmes mondatok része, mondjuk: Három morcona kal**ÓZ Ő**rzi a kincset a szigeten... vagy: Szörny**Ű ÉH**ség gyötörte... De ez igazából nem vezet sehova, inkább fordítsuk figyelmünket a fennmaradó számokra.

$$36,\ 44,\ 120,\ 68,\ 24,\ 36,\ 12,\ 16,\ 20,\ 32,\ 168,\ 48.$$

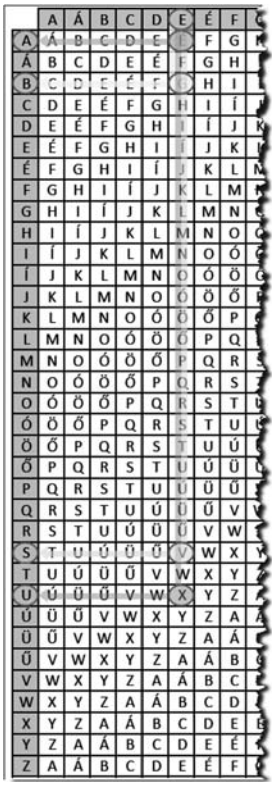
És igen, a többi távolság mind a 4 szám többszöröse, vagyis az ismétlődések 9-szer, 11-szer, 30-szor, 17-szer stb. 4 betűnyire követik egymást, és ez csak azt jelentheti, hogy a kulcs négy karakterből áll.

Ezzel még egyáltalán nem vagyunk kisegítve, hiszen rengeteg négybetűs szó van, ki állna neki mindet végigpróbálni. Szerencsére nem is kell.

Ne akarjuk újra feltalálni a kereket!

Nézzük ezt az eredményt más szemüvegen keresztül. Az, hogy a kulcs hossza 4, azt jelenti, hogy a szöveg minden negyedik betűjét azonos kulcsbetűvel kódoltuk, a mi példánknál az 1., 5., 9., 13., ... betűt B szerint, a 2., 6., 10., 14., ... betűt U szerint, a 3., 7., 11., 15., ... betűt S szerint, végül a 4., 8., 12., 16., ... betűt A szerint.

Igen, ez a négy csoport monoalfabetikus kódolású. Ha összeválogatjuk a betűket, mind a négy csoportban végezhetünk gyakorisági vizsgálatot. Szerencsére most csak a leggyakoribb jelet kell megkeresni a négy csoportban, a mi példánknál maradva ez legyen G, X, V és É, vagyis rendre ezek a jelek fordulnak elő legtöbbször az első, a második, a harmadik és a negyedik csoportban.



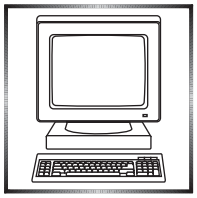
Ha ezek vannak az egyes csoportok gyakorisági táblázatának élén, akkor ezekké kódolódott a magyarban leggyakoribb betű, az E. Nézzük meg a Vigenére-tábla E oszlopát és keressük meg, melyik sorokban találjuk ezeket a betűket:

a G-t	a B oszlopban;
az X-et	az U oszlopban;
a V-t	az S oszlopban, végül
az É-t	az A oszlopban.

A kapott betűket a fenti sorrendben már csak össze kell olvasnunk és meg is van a kulcs: BUSA. A kulcs ismeretében alig valamivel nehezebb kihámozni a titkos üzenet értelmét, mintha a kódolatlan üzenetet nyomták volna a markunkba.

Végkövetkeztetésül: Ha elég hosszú a szöveg, továbbá ismerjük az adott nyelv leggyakrabban használt betűjét, akkor bizony a Vigenère-kódolású üzenet is megfejthető a kulcs ismerete nélkül. Babbage munkája új kihívás elé állította a rejtjelezőket, így született meg az ENIGMA, az RSA és az MD5 kódolás, de ez már egy másik történet. Hiábavaló volt tehát a sok fáradság, amivel kitalálták e furfangos titkosítási módszert, és a kódolásra fordított energia is kárba veszett a zseniális elmével szemben, és ez így volt törvényszerű. Hiszen kell lennie valamilyen értelmes rendszernek a kódoláskor, mert ha például a Bibliát szeretnénk titkosítani, mondjuk úgy, hogy ábécébe rendezzük a szavait, akkor sem lehetnénk biztosak benne, hogy némi próbálkozás után az eredeti szöveget kapjuk vissza. A Vigenère-módszer utódai is megfejtve végezték, vagy végzik majd.

Tóth Tamás



Informatikából kitűzött feladatok

I. 547. A morzekód (Samuel Morse találmánya) olyan kommunikációs kód, amely pontok és vonalak kombinációjából áll. Szöveges üzenet átvitelére alkalmas vezetékes, vagy vezeték nélküli kommunikációs csatornán.