Üzenetek titkosítása az óra-aritmetika alkalmazásával

Catherine A. Gorini[1]

A számítógépek és más elektronikus kommunikációs eszközök befolyással vannak életünk szinte minden területére az áruházi vásárlástól kezdve a DNS szerkezetének, vagy éppen a világegyetem eredetének megértéséig. Ilyesfajta szerkezetek alkalmazásához azonban elengedhetetlen a nagy adathalmazok tárolása, továbbítása és persze megértése, áttekinthetővé, olvashatóvá tétele. A kódelmélet és kriptográia feladata, hogy az ilyen adathalmazok kezelésének két alapvető feltételét, vagyis az adatok titkossá tételét és továbbításuk precízségét biztosítsa. Ez a cikk egy olyan órai foglalkozást mutat be, melyben a diákok, egymásnak titkos üzeneteket küldve a számelméletnek egy gyakorlati alkalmazását fedezhetik fel. Ezen elfoglaltság megvilágítja, hogy miért van szükség a hatványkitevőkre vonatkozó törvényszerűségek vizsgálatára a számoló- vagy számítógépes számolások lehetővé tételéhez, és tökéletes módszer a kitevők törvényeinek felvázolására, újfajta alkalmazásaik megértésére, megtanulására.

A különböző hadseregek és kormányok már évezredek óta használnak titkos kódokat, sifréket, de manapság egyre inkább elterjedtek az iparban, az üzleti életben és az otthoni PC-ken is. Példának okáért egy bankban szükség lehet rá, hogy az adatokat a központi irodából az egyes bankfiókokba a telefonvonalakon keresztül küldjék el. Azonban a telefonvonalak lehallgathatóak, a bank által közvetített adatok pedig bizalmasak, nem kerülhetnek idegen kezekbe. A kriptográfia, a titkos kódok alkalmazásának tudománya azt hivatott biztosítani, hogy csak az eredeti címzett számára legyen érthető az üzenet.

Kódok széles körben használatosak az üzleti életben, az ipar és a kormányzás területén.

A legősibb kódok azon alapultak, hogy az üzenetben minden betűt vagy számot egy másik betűvel vagy számmal helyettesítettek egy, csak a feladó és a címzett által ismert kulcs szerint. A legújabb sifrék, melyeknek alkalmazásához nagysebességű számítógépekre van szükség, számelméleti és oszthatósági aritmetikai elveken alapulnak. Az új kódok, melyeket *nyilvános kódú titkosírásoknak* is nevezünk, olyan kulcsot, kódolási rendszert használnak, melyet a címzett nyilvánosságra hoz. Az ilyenfajta kódokat hívják *csapóajtó-sifréknek* is, mert bár az üzenetek titkossá tételének módja ismert, feltörni őket gyakorlatilag lehetetlen. Ezek működési alapja, hogy egyszerűen elvégezhető aritmetikai műveletek fordítottjai nehezen hajthatók végre. Példának okáért két nagy szám viszonylag könnyen összeszorozható, de egy nagy számot tényezőkre bontani már sokkal nehezebb.

Ez a cikk bemutatja az oszthatósági aritmetikát és a számelméletnek néhány ezzel foglalkozó tételét, leírja az 1978-ban a MIT-en Ronald L. Rivest, Adi Shamir és Leonard Adleman által kifejlesztett RSA nyilvános kulcsú titkosírásrendszert,

[1]Cathy Gorini, cgorini@mum.edu, a Maharishi University of Management, Fairfield, IA 52557. tanára.

valamint körvonalaz egy foglalkozást, amely felhasználja ezt a rendszert. A legutolsó részben néhány, a továbbiakban tanulmányozható téma található.

Oszthatósági aritmetika

Az oszthatósági aritmetika fontos része a számelméletnek és absztrakt algebrának. Az aritmetika ezen ágával először a tizenkilencedik század elején foglalkozott Carl Friedrich Gauss (1777-1855), mint a számok oszthatóságának vizsgálatára alkalmas elmélettel. Az oszthatósági aritmetika nevezhető óra-aritmetikának is, mert a számok összeadása modulo 12 (a 12-vel osztva adott maradék szerint) megfelel a számok összeadásának egy tizenkét órás óra számlapján. Az oszthatósági aritmetikának egy közismert alkalmazása, mikor az egészekkel végzett műveletek ellenőrzéseképpen ellenőrizzük az eredmény 9-es maradékát. Az oszthatósági aritmetikában választandó egy pozitív egész n mint a kongruenciák alapja. Egy egész szám redukálása modulo n azt jelenti, hogy a számot helyettesítjük n-nel osztva adott maradékával. Ennek alapján 38 redukálása modulo 12, 2-t eredményez. A művelet a következőképpen formalizálható:

$$38 \equiv 2 \bmod 12$$

vagyis "38 kongruens 2-vel mod 12." Ha a kongruencia alapját a szövegkörnyezet egyértelművé teszi, írhatunk $38 \equiv$ 2-t is. Az összeadás, kivonás vagy szorzás mod$n$ elvégzésekor a művelet eredményének n-nel osztva adott maradékát kell venni. $7 + 9$ kiszámolásakor például az eredmény 4, mivel $7 + 9 \equiv 4 \bmod 12$. Az órás hasonlattal élve kilenc órával hét óra után éppen négy óra van.

Egy hosszabb műveletsor elvégzésekor azonkívül, hogy a végeredményt redukáljuk mod$n$, megtehetjük, hogy a számolás során tetszőlegesen néhány részeredményt n-nel osztva adott maradékával helyettesítünk. Rengetegféleképpen kiszámolhatjuk például a $(15 \times 27) + 57$ művelet eredményét (mod 12). Elvégezve a szorzást majd az összeadást 462-t kapunk, melynek 12-es maradéka 6. A szorzás eredményének (405) 12-es maradéka 9, $9 + 57 = 66$ 12-es maradéka pedig 6. A lehető legegyszerűbben pedig, először redukálva mindhárom számot mod12, az eredmény megintcsak $(3 \times 3) + 9 = 18 \equiv 6 \bmod 12$.

Ha a diákok rendelkeznek TI Math Explorer-rel, könnyen meghatározhatják egy x szám n-nel osztva adott maradékát. Egyszerűen begépelik a következőt: $\boxed{x}$ $\boxed{\text{INT+}}$ $\boxed{n}$ $\boxed{=}$ és tekintik a maradékot. Más számológépekkel dolgozva x-et elosztják n-nel, majd a hányadosból egészrészét kivonva az eredményt megszorozzák n-nel. A számológéppel kapott eredmény rendszerint egész, de ha nem az, akkor is nagyon közel van egy egészhez és könnyen kerekíthető. Példának okáért $5378 = (448 \times 12) + 2$, vagyis $5378 \equiv 2 \bmod 12$. Számológéppel számolva, $5378 \div 12 = 448,16667$. $448,16667 - 448 = 0,16667$. Ezt a számot 12-vel megszorozva $1,9999999$-et kapunk, mely a legközelebbi egészre kerekítve 2. Meg

kell jegyeznünk, hogy $448,16667$-ból levonni egészrészét gazdaságosabb, mint begépelni $0,16667$-t, egyrészt, mert kevesebb gépelésünkbe kerül, másrészt pedig, mert így megőrizzük a kalkulátor memóriájában tárolt további tizedesjegyeket.

Az RSA kódolási rendszer használatához szükséges számításokban gyakran szerepelhetnek nagy számok magas kitevőkkel. Egy számológépnek esetleg nincs ilyen nagy számokkal való munkához elegendő memóriája. A kitevők törvényszerűségeinek alkalmazásával azonban egy művelet néhány közbenső lépés beiktatásával leegyszerűsíthető annyira, hogy egy számológép is megbirkózzon vele.

Próbáljuk meg például számológéppel kiszámolni $7^{26} \bmod 12$ értékét. A gép hatványozó funkcióját használva (amelyhez leggyakrabban $\boxed{x^y}$ vagy $\boxed{y^x}$ jelű gomb, billentyű tartozik) $9,3874803 \times 10^{21}$-t kapunk eredményül, amely egy kerekített érték. Az oszthatósági aritmetikában azonban, eltérően másféle számításoktól itt semmi hasznát nem vesszük az ilyesfajta kerekített értékeknek. Egy pontos egész értékre van szükség, mivel bármelyik jegy kicserélése megváltoztathatja az eredményt. Mit tehetünk? A kitevők törvényszerűségei szerint $x^{a+b} = x^a \cdot x^b$ és $x^{a \cdot b} = (x^a)^b$. Ezen szabályok segítségével a magas kitevőt tartalmazó számolás felbontható több, kisebb kitevővel számoló feladatra. Ezen törvényeket alkalmazva 7^{26}-ra (és a részeredményeket redukálva mod12 amikor ez megkönnyíti a számolást) a következőképpen járhatunk el:

$$\begin{aligned} 7^{26} &= 7^2 \cdot 7^{24} \\ &= 7^2 \cdot \left(7^4\right)^6 \\ &= 49 \cdot (2401)^6 \\ &\equiv 1 \cdot (1)^6 \bmod 12 \\ &\equiv 1 \end{aligned}$$

Természeten a kitevők szabályait sokféleképpen alkalmazhatjuk ugyanazon művelet elvégzésének megkönnyítésére. A fenti számolást például a következőképpen is végrehajthattuk volna:

$$\begin{aligned} 7^{26} &= \left(7^2\right)^{13} \\ &= (49)^{13} \\ &\equiv (1)^{13} \bmod 12 \\ &\equiv 1 \end{aligned}$$

Számológéppel dolgozva a lehető legjobb eredmények eléréséhez kérjük meg a diákokat, hogy számításaikban használjanak elegendően kicsi kitevőket ahhoz, hogy a számológép a részeredményeket rendes alakjukban, és ne normálalakban határozza meg; az utóbbi formában közölt eredmények azt mutatják, hogy a kalkulátor memóriája nem elég nagy ahhoz, hogy a gép a teljes választ kiírja. Ez a későbbi számolásoknál problémát okozhat.

A megfelelő köztes kitevők megtalálásához némi tapasztalat szükséges, de ebben segítségünkre lehet néhány durvább becslés. Mivel 10^n-nek $n+1$ jegye van, és bármelyik, ennél kisebb számnak (legfeljebb) n jegye van, egy olyan számológépen, amely legfeljebb 8 jegyű számokat képes kiírni, 10-nél kisebb számokat olyan kitevővel használjunk, amely 8-nál kisebb, vagy éppen 8. 20^6 pont 8-jegyű, ezért a számokat 20-ig emelhetjük hatodik hatványra. 30-ra az 5-nél kisebb, vagy 5-tel egyenlő együtthatókra kaphatunk pontos eredményt.

Kezdjük két nagy prímszám szorzatának kiszámításával!

A csapóajtó-sifrék alkalmazásával az egyes üzenetek titkosításához és olvasásához szükséges számolások remek alkalmat biztosítanak a diákoknak, hogy felfedezzék azokat a módszereket, amelyek a kitevőkkel kapcsolatos szabályok segítségével egyszerűsítik le az oszthatósági aritmetikai műveletek elvégzését számológéppel. Az oszthatósági számításokban ezeket az egyszerűsítéseket használják a számítógépek is.

Néhány számelméleti tétel

Az RSA titkosírás-rendszer egy oszthatósági aritmetikáról szóló tételen, Euler tételének egy speciális esetén alapszik. A tételt a svájci matematikus, Leonhard Euler (1707-1783) bizonyította be. Ez a tétel egy másikra épül, amelyet a franica matematikus, Pierre de Fermat (1601-1665) bizonyított be, és amelyet (megkülönböztetésül Fermat híresebb, utolsó tételétől) 'kis Fermat-tétel'-nek nevezünk.

1 Tétel (A kis Fermat-tétel)
Tetszőleges a egész számra, ha p prím, akkor $a^p \equiv a \bmod p$.

A diákok számológépük segítségével ellenőrizhetik a tételt különböző a és p értékekre. Ez az elfoglaltság lehetőséget nyújt nekik, hogy oszthatósági aritmetikával és hatványozással foglalkozzanak számológép használatával, és meggyőzi őket arról, hogy Fermatnak eme figyelemre méltó tétele igaz. Megjegyzendő, hogy ha a kisebb, mint p, akkor $a^p \bmod p$ éppen a-val egyenlő, ha pedig a nagyobb, mint p, akkor a-t és a^p-t redukálnunk kell $\bmod p$ hogy egyenlő számokat kapjunk. Euler tételének a későbbiekben használt speciális esete a következő:

2 Tétel
Ha p és q prímek és k olyan egész, melyre teljesül, hogy

$$k \equiv 1 \bmod (p-1)(q-1),$$

akkor

$$a^k \equiv a \bmod pq\ .$$

A diákok ezt a tételt is ellenőrizhetik kis számhármasokra, például $p=3$, $q=5$ és $k=9$ vagy $p=3$, $q=7$ és $k=13$.

Az RSA nyilvános kulcsú titkosírásrendszer

Az RSA titkosírásrendszert használva az üzenet címzettje választ két nagy p és q prímet, kiszámítja szorzatukat, $n = p \cdot q$, majd keres egy k egészt, ami 1 maradékot ad $(p-1)(q-1)$-gyel osztva. Ha k felbontható két egész, E (az encoding, vagyis titkosítás szóból) és D (a dekódolás szóból) szorzatára, akkor bármely a egészre

$$a^k = \left(a^E\right)^D \equiv a \bmod n$$

G.H. Hardy még azt gondolta, hogy a számelméletnek semmilyen praktikus alkalmazása nem lehetséges.

Bárkinek, aki üzenetet akar neki küldeni, a címzett megadja az n és E értékeket, azzal az utasítással, hogy az üzenet n-nél kisebb számok sorozata legyen. A feladó az üzenetben minden számot E-edik hatványra emel, majd a hatványt $\bmod n$ redukálja. Az így kapott számokat küldi el a címzettnek. Amikor a címzett megkapja a titkosítás utáni számsorozatot, abban minden számot D-edik hatványára emel, és veszi a hatvány n-nel osztva adott maradékát. Az eredmény az eredeti, titkosítás előtti számsorozat.

Például, ha a címzett a $p = 2$ és $q = 11$ prímeket választja, akkor k értékére igaz, hogy

$$k \equiv 1 \bmod (2-1)(11-1)$$

vagyis

$$k \equiv 1 \,(\mathrm{mod} 10)$$

Itt k értékének felbonthatónak kell lennie 1-en és k-n kívül két egész szorzatára. a 10-zel osztva 1 maradékot adó számok 1, 11, 21, 31, 41 és így tovább. A legkisebb ilyen nem prím szám (ami nem az 1-es, vagyis szorzattá bontható) a 21, ezért a k értékének a 21-et választjuk, és 3 és 7 szorzatára bontjuk. Legyen $E = 7$ és $D = 3$. Ez azt jelenti, hogy a feladónak az üzenetben szereplő minden számot 7-edik hatványára kell emelnie, majd a hatványt redukálnia kell mod$n = 22$. Tegyük fel, hogy valaki a '14' üzenetet szeretné elküldeni. A feladó a pontos eredmény eléréséhez köztes kitevőkkel számol,

$$\begin{aligned} (14)^7 &= (14)^3 \cdot (14)^4 \\ &= 2744 \cdot 38416 \\ &\equiv 16 \cdot 4 \bmod 22 \\ &\equiv 20 \end{aligned}$$

és elküldi a '20' üzenetet. Mikor az üzenet megérkezik, a címzett a következőképpen számol:

$$\begin{aligned} (20)^3 &= 8000, \\ 8000 &\equiv 14 \bmod 22 \end{aligned}$$

És így megkapja az eredeti üzenetet.

A valóságban az RSA rendszer használatakor a választott p és q prímek száz, vagy még annál is több jegyűek; hatékony, számelméleti alapokon nyugvó számítógépes algoritmusok gyorsan találnak ilyeneket. Ilyen prímekkel a kongruenciák alapja, $n = pq$, amelyet nyilvánosságra hoznak, legalább kétszáz jegyű szám lesz. Mivel a jelenlegi technológia mellett a leghatékonyabb számítógpes programoknak is évmilliárdokig tartana tényezőkre bontani egy 200 jegyű számot, és mivel a titkosításhoz szükséges E szám ismerete semmilyen értékes információt nem ad n faktorizálásához, ezek a sifrék nagyon biztonságosak. Ugyanakkor a gyors oszthatósági aritmetikai számítógépes algoritmusok alkalmassá teszik ezt a titkosírás-rendszert a mindennapi használatra.

A Foglalkozás

Az ebben a részben található javaslatok segítségével a diákok az RSA-rendszer szerint titkosított üzeneteket küldhetnek egymásnak n, E és D kis értékeit használva. Ez a foglalkozás lebonyolítható körülbelül két óra alatt, feltéve, hogy a diákok értik az oszthatósági aritmetikát, alkalmazni tudják a kitevőkkel kapcsolatos szabályokat és számológépükkel meg tudják határozni egészeknek egy másik egésszel osztva adott maradékát. A foglalkozás lebonyolításához szükség van arra is, hogy a diákok rendelkezzenek számok hatványozására alkalmas számológéppel, mint például a TI Math Explorer vagy más tudományos kalkulátor. A tanárnak a titkosítás és dekódolás több példáját is át kell vennie az osztállyal, mielőtt hagyja, hogy a diákok a saját üzeneteiket küldjék el. Az "Egy mintaüzenet elküldése" rész egy, az osztállyal átvehető példát mutat be.

Az osztály kisebb csoportokra osztható úgy, hogy minden csoport kapjon egy számot, amely egy sifrének felel meg 1. táblázatból. A csoportok ezután az ő számuknak megfelelő sifrét használják majd. Minden csoport készíthet magának egy kártyát, rajta a számával, de a táblára is felírhatjuk sorban a csoportvezetők nevét csoportjuk sifréjének számával együtt. Minden csoport megkapja az első táblázatban található adatokat.

Ezután a diákok megpróbálhatnak üzeneteket küldeni egymásnak. Kezdetnek jó, ha egy csoport csak egyszámos üzeneteket küld. Ehhez minden csoportnak ki kell választania egy másikat, amellyel együttműködhet és egy számot vagy üzenetet, amelyet elküldhet. Az üzenet elküldéséhez a benne szereplő számokat E-edik hatványukra emelnie és az eredményt mod$n$ redukálnia kell, az általuk kiválasztott csoport sifréjének E és n értékeit használva. Az így kapott végső értéket vagy értékeket egy darab papírra írva elküldhetik a másik csapatnak.

Ha egy csoport üzenetet kap, szeretné majd megfejteni és az eredményt egyeztetni az üzenetet küldő csoporttal, hogy jó eredményre jutott-e. A tanárnak minden csoportnak meg kell adnia a számához tartozó D értéket a második táblázatból, amit a csoport aztán felhasználhat a kapott üzenetek dekódolására.

1. sifre	$n = 55$	$E = 23$
2. sifre	$n = 65$	$E = 29$
3. sifre	$n = 85$	$E = 13$
4. sifre	$n = 77$	$E = 37$
5. sifre	$n = 91$	$E = 29$
6. sifre	$n = 95$	$E = 31$
7. sifre	$n = 119$	$E = 35$
8. sifre	$n = 161$	$E = 19$
9. sifre	$n = 253$	$E = 17$
10. sifre	$n = 133$	$E = 25$
11. sifre	$n = 145$	$E = 25$
12. sifre	$n = 185$	$E = 29$

1. táblázat. Titkosító kódok

A D szám titokban tartható, ha a tanár minden csoportnak egy összehajtott papírdarabkára írva adja oda.

1.sifre	$D = 7$
2.sifre	$D = 5$
3.sifre	$D = 5$
4.sifre	$D = 13$
5.sifre	$D = 5$
6.sifre	$D = 7$
7.sifre	$D = 5$
8.sifre	$D = 7$
9.sifre	$D = 13$
10.sifre	$D = 13$
11.sifre	$D = 9$
12.sifre	$D = 5$

2. táblázat. Dekódok

Minden csapat feladata, hogy üzeneteket küldjön a többi csapatnak és a kapott üzeneteket megfejtse. Ha a diákok már elég gyakorlottak a számolási módszerek használatában, képesek lesznek arra, hogy teljes szavakat, vagy akár mondatokat üzenjenek. Egész mondatos üzenetek készítésénél célszerű, ha a csoport minden tagja a mondatnak más-más betűjét kódolja, majd a csoport egy másik tagjának munkáját ellenőrzi. A harmadik táblázat arra mutat egy lehetőséget , hogy hogyan alakítsuk a szavavat számokból álló üzenetté.

Az első táblázatbeli sifrék durván nehézségi sorrendben vannak. A dekódoló eljárás, D-edik hatványra emelés mindegyik sifrében egyszerűbb, mint az üze-

net titkosítása, vagyis E-edik hatványra emelés, mivel a diákok által küldött üzenetekben szereplő számok 1 és 26 között lesznek. A kódolás során kapott számok meglehetősen nagyok is lehetnek, és ha csak alacsonyabb hatványra kell őket emelni, az egyszerűsíti a megfejtés folyamatát. A foglalkozást játékként is játszhatjuk, ha pontot adunk minden titkosított vagy megfejtett üzenet után.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

3. táblázat. Számkódok az ABC betűire

Számítási technikák

Az ebben a gyarkorlatban végzett számítások könnyen elvégezhetőek a TI Math Explorer számológéppel, ami rendelkezik hatványozó billentyűvel és nyolc számjegyet tud kiírni. A TI Math Explorer-nek az egész számokkal adott maradékot számító funkciója csak négyjegyűnél kisebb hányadosokkal és maradékokkal tud dolgozni, ezért ha a diákok ezt használják a számok redukálására, kisebb köztes kitevőket kell használniuk. A több kijelzősoros TI-82 grafikus kalkulátor ideális a számok oszthatósági aritmetikai redukálására, mivel a számológép a korábbi számítások eredményeit is mutatja. Tehát ahhoz, hogy egy számnak törtrészét vegyük, nincs szükség arra, hogy a számból kivonandó egészrészt fejben tartsuk vagy leírjuk.

Jobb, ha a diákok elég kis kitevőket használnak ahhoz, hogy az eredményeket számológépük teljesen kiírja; túl bonyolult normál alakú számokkal dolgozni, még akkor is, ha a számológép memóriájában tárolt számjegyekre hagyatkozunk.

Az alkalmazások az elektronikus kommunikáció területén meglepőek lehetnek.

A műveletek sorrendje nagyon fontos. Például ahhoz, hogy kiszámoljuk 31 3-as maradékát, a következő műveletsort kell elvégeznünk: $((31 \div 3) - 10) \times 3 = 1$. A legtöbb számológépen meg kell nyomnunk az $\boxed{=}$-t vagy az **ENTER**-t a $\boxed{\times}$ megnyomása előtt ahhoz, hogy a számológép előbb végezze el a kivonást, mint a szorzást. Ha a diákok nem ismerik a műveletek sorrendjét az ő számológépükön, jobb, ha $\boxed{=}$-t vagy **ENTER**-t nyomnak minden egyes művelet elvégzése után.

Ha sok számot ugyanazon szabály szerint akarunk kódolni, akkor egyszerűbb, ha először a 26-nál kisebb prímeket kódoljuk. Ezután az összetett számok titkosítása már kevésbé bonyolult az $(xy)^a = x^a y^a$ szabály szerint. Példának okáért, ha tudjuk, hogy

$$2^{23} = 8388608 \equiv 8 \bmod 55$$

és

$$\begin{aligned} 3^{23} &= \left(3^{10}\right)^2 \cdot 3^3 = 59049^2 \cdot 27 \equiv \\ &\equiv 34^2 \cdot 27 \equiv 1 \cdot 27 \equiv 27 \bmod 55 \end{aligned}$$

akkor 6^{23} és 8^{23} egyszerűen kiszámolható a következőképpen:

$$6^{23} = 2^{23} \cdot 3^{23} \equiv 8 \cdot 27 \equiv 51 \bmod 55$$

és

$$8^{23} = \left(2^3\right)^{23} = \left(2^{23}\right)^3 \equiv 8^3 \equiv 17 \bmod 55$$

Egy mintaüzenet elküldése

Legyen az üzenet, amit el akarunk küldeni "szervusz", és használjuk az 1. táblázatban szereplő 1. sifrét. A harmadik táblázat szerint ennek az üzenetnek a $19-26-5-18-22-21-19-26$ számsorozat felel meg. Ezeket a számokat a következőképpen kódolhatjuk:

$$\begin{aligned} 19^{23} &= \left(19^2\right)^{11} \cdot 19 = 361^{11} \cdot 19 \equiv 31^{11} \cdot 19 \equiv \\ &\equiv \left(31^5\right)^2 \cdot 31 \cdot 19 \equiv 1^2 \cdot 31 \cdot 19 \equiv 39 \bmod 55 \end{aligned}$$

$$26^{23} = \left(26^5\right)^4 \cdot 26^3 \equiv 1^4 \cdot 17576 \equiv 31 \bmod 55$$

$$5^{23} \equiv 15 \bmod 55$$

$$18^{23} = (2 \cdot 3 \cdot 3)^{23} = 2^{23} \cdot 3^{23} \cdot 3^{23} \equiv 8 \cdot 27 \cdot 27 \equiv 2 \bmod 55$$

$$22^{23} = (2 \cdot 11)^{23} = 2^{23} \cdot 11^{23} \equiv 8 \cdot 11 \equiv 33 \bmod 55$$

$$\begin{aligned} 21^{23} &= (3 \cdot 7)^{23} = 3^{23} \cdot 7^{23} \equiv 27 \cdot \left(7^6\right)^3 \cdot 16807 \equiv \\ &\equiv 27 \cdot 9 \cdot 32 \equiv 21 \bmod 55 \end{aligned}$$

A titkosított üzenet tehát $39-31-15-2-33-21-39-31$ lesz, amit a címzett az alábbi módon dekódol:

$$39^7 = \left(39^2\right)^3 \cdot 39 \equiv 36^3 \cdot 39 \equiv 16 \cdot 39 \equiv 19 \bmod 55$$

$$31^7 = \left(31^2\right)^3 \cdot 31 \equiv 26^3 \cdot 31 \equiv 31 \cdot 31 \equiv 26 \bmod 55$$

$$15^7 = \left(15^2\right)^3 \cdot 15 \equiv 5^3 \cdot 15 \equiv 5 \bmod 55$$

$$2^7 = 128 \equiv 18 \bmod 55$$

$$33^7 = \left(33^2\right)^3 \cdot 33 \equiv 44^3 \cdot 33 \equiv 44 \cdot 33 \equiv 22 \bmod 55$$

$$21^7 = \left(21^2\right)^3 \cdot 21 \equiv 1^3 \cdot 21 \equiv 21 \bmod 55$$

A címzett tehát hozzájut az eredeti üzenethez, ami $19-26-5-18-22-21-19-26$, vagyis 'szervusz'.

Ajánlatok a téma további tanulmányozásához

A kriptológia iránt érdeklődő diákok bizonyára érdekesnek találják majd Kahn (1967) és Sinkov (1966) könyveit. Hellman (1979) azt tárgyalja, hogy hogyan jelenthet az RSA-rendszer védelmet a hamisítás ellen. A DES-ről (Data Encryption Standard) olvasva a diákok érdeklődését felkeltheti a technológia hatása a politikára. A DES titkosírás-rendszert a National Bureau of Standards fejlesztette ki ("Debating Encryption Standards" 1992; Markoff 1992)

Összefoglalás

A számelmélet ezen alkalmazásai az elektromos kommunikáció terén meglepőnek tűnhetnek, különösen a számelméletet megalkotó matemetikusok szemében. A 20. század elejének nagy számelmélésze, G. H. Hardy (1877-1947) például meg volt róla győződve, hogy az aritmetikának semmiféle gyakorlati haszna nincs. Hardy (1976, 101-102) művében, melyben a $\sqrt{2}$ irracionalitását és a prímek számának végtelenségét (azt a tényt, ami működőképessé teszi az RSA-rendszert) tárgyalja, a következő véleményt fogalmazza meg:

> Egyik tétel "komolyságához" sem fér kétség. Ezért nem árt megjegyezni, hogy egyik tételnek sincs a leghalványabb gyakorlati jelentősége sem. A gyakorlati alkalmazásokban általában csak viszonylag kis számokkal kell foglalkoznunk; csak a csillagászat és az atomfizika dolgozik "nagy" számokkal, és ezeknek —egyenlőre— alig van több gyakorlati jelentősége, mint a legelvontabb színtiszta matematikának. Nem tudom, hogy a pontosságnak mely fokára lesz egy mérnöknek valaha szüksége —nagyon nagyvonalúak vagyunk, ha ezt 10 érték-számjegyre becsüljük. Ekkor
>
> $$3,14159265 = \frac{314159265}{1000000000}$$
>
> (π értéke a nyolcadik tizedesjegyig) két legfeljebb 10-jegyű szám hányadosa. 50847478 prím van, amely kisebb, mint 1000000000: egy mérnöknek elég ennyi, és tökéletesen boldog lehet a többi nélkül.

Az RSA nyilvános kulcsú titkosírásrendszer a száz, vagy még több jegyű prímekre épül, cáfolva Hardy megállapításait a számelmélet hasznosságára vonatkozóan. Az emberi képzelet esélyes arra, hogy hasznosítsa a matematikai tudást az élet különböző területein, és mi, mint tanárok kihívásul állíthatjuk diákjaink elé, hogy a még megoldatlan problémákat a matematika új alkalmazásaival hidalják át.

Hivatkozások

[1] "Debating Encryption Standards." Communications of the Assotiation for Computing Machinery 35 (1992 július): 33-34.

[2]Hardy, Geoffrey H. A Mathematician's Apology. Cambridge: Cambridge University Press, 1976.

[3]Hellman, Martin. "The Mathematics of Public Key Cryptography." Scientific American 241 (1979 augusztus): 146-57.

[4]Kahn, David. The Codebreakers. New York: Macmillan Publishing Co., 1967.

[5]Markoff, John. "Software Coding for Export: Security Agency and Industry in Talks." New York Times, 1992 március 24., C1, C15.

[6]Sinkov, Abraham. Elementary Cryptanalysis. Washington, D.C.: Mathematical Assotiation of America, 1966.

Bibliográfia

Bennett, Charles H., Gilles Brassard, és Arthur K. Ekert. "Quantum Cryptography" Scientific American 267 (1992 október): 50-57.

Gardner, Martin. Penrose Tilings to Trapdoor Ciphers. New York: W. H. Freeman & Co., 1989.

Lefton, Phyllis. "Number Theory and Public-Key Cryptography." Mathematics Teacher 84 (1991 január): 54-62.

Malkevitch, Joseph, Gary Froelich, and Daniel Froelich. Codes Galore. Arlington, Mass.: COMAP, 1991.

Markoff, John. "Scientists Devise Math Tool to Break a Protective Code." New York Times, 1991. október 3, A16.

Ore, Oystein. Number Theory and Its History. New York: Dover Publications, 1990.

Rivest, Roland L., Adi Shamir és Leonard Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the Assotiation for Computing Machinery 21 (1978 február): 120-26.

Stewart, Ian. The Problems of Mathematics. Oxford: Oxford University Press, 1987.

Thompson, Thomas M. From Error-Correcting Codes to Sphere Packings through Simple Groups. Washington D. C.: Mathematical Assosiation of America, 1983.

Wood, Eric F. "Applications: Self-Checking Codes—an Application of Modular Arithmetic." Mathematics Teacher 80 (1987 április): 312-16.

Wright, Marie A. "Conventional Cryptography." Mathematics Teacher 86 (1993 március): 249-51.

Fordította: *Puskás Anna*