Pierre Fermat (1601–1665) pontosan 100 évvel Girolamo Cardano (1501–1576) születése után, 1601-ben született.

A következőkben a nevéhez kötődő kis Fermat-tételről lesz szó, amelynek jelzője ellenére alapvető hatása van napjaink információ-titkosítására. Fermat eredeti tételét ma a következő formában mondjuk ki:

Kis Fermat-tétel: *Ha p prímszám és a nem osztható p-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

(A kongruencia[1] $a \equiv b \pmod{c}$, amit a kongruens b modulo c-nek olvasunk, és azt jelenti, hogy ha a-t és b-t a c-vel osztjuk, akkor egyenlő maradékot kapunk, azaz $a = xc + b$, ahol x egész szám. fogalmát Gauss vezette be.)

Fermat bizonyítása azonban ebben az esetben sem maradt fenn. Az első bizonyítás majd 100 évig váratott magára és Leonhard Eulertől (1707–1783), a XVIII. század matematikus óriásától származik. Euler egyben a tétel általánosítását is bebizonyította, így ma Euler–Fermat-tételnek nevezzük:

Euler–Fermat-tétel: *Ha $m > 1$ egész szám és $(a,\ m) = 1$, azaz a és m relatív prímek,[2] Két egész számot (például a és m) relatív prímnek mondunk, ha 1-en kívül nincs közös pozitív osztójuk. Jelölése: $(a,\ m) = 1$. akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{2}$$

A tételben szereplő Euler-féle $\varphi(m)$ függvény jelenti az 1, 2, ..., m számok közül az m-hez relatív prímek számát. Például: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$ ...

Általában igaz, hogy ha $m = p$ prímszám, akkor

$$\varphi(p) = p - 1. \tag{3}$$

Ebből az is könnyen belátható, hogy ha p és q különböző prímek, akkor

$$\varphi(pq) = (p-1)(q-1). \tag{4}$$

A prímszámoknak és a számok osztóinak fontos jelentést tulajdonítottak az ókori számmisztikában olyannyira, hogy Pithagorasz és követői, (i.e. VI–V. század), úgy tartották, hogy „*A dolgok természete, lényege: a szám.*" De nemcsak hirdették, hanem szerintük a természeti és társadalmi jelenségeket valóban a számok csodálatos tulajdonságai „testesítették meg". A pitagoreusok ugyanis nem a számokat személyesítették meg, hanem – többek között – a személyes (emberi) tulajdonságokat „számosították meg".

Tökéletesnek tartottak például egy számot, ha az megegyezett a nála kisebb pozitív osztóinak összegével. Tökéletes számok[3]Már Euklidesz (i.e. 300 körül) jellemezte a páros tökéletes számokat: *Ha $1+2+\cdots+2^n = 2^{n+1}-1$ prímszám (azaz 1-en és önmagán kívül nincs más pozitív osztója), akkor $2^n(2^{n+1}-1)$ tökéletes szám, és minden páros tökéletes szám ilyen alakú. Nem ismeretes páratlan tökéletes szám.* a $6 = 1+2+3$ és a $28 = 1+2+4+7+14$. A pitagoreusok csak néhány tökéletes számot ismertek, így a 496-ról és a 8128-ról is tudtak. A matematikusok az ókor óta nem tudják, hogy van-e végtelen sok tökéletes szám. Az ötödik tökéletes számot, a 33 550 336-ot a XV. században találták meg, míg a XVI. század adta a hatodik és hetedik tökéletes számot, ezek a $2^{16}(2^{17}-1)$ és a $2^{18}(2^{19}-1)$. Látható, hogy amint a tökéletes számok között haladunk „előre", egyre nagyobb távolságok vannak, így nem meglepő, hogy egyre nehezebb újabb tökéletes számokat találni. A nyolcadik tökéletes szám megtalálására a XVIII. századig kellett várni, amikor Leonhard Euler kimutatta, hogy a $2^{30}(2^{31}-1)$ is tökéletes szám. A számítógépek megjelenéséig még négy tökéletes számot sikerült megtalálni a XIX. században kézi számolással, ezek a $2^{60}(2^{61}-1)$, $2^{88}(2^{89}-1)$, $2^{106}(2^{107}-1)$ és a $2^{126}(2^{127}-1)$.[4]Ezek leírásához a tízes számrendszerben 40, 60, 80 számjegyre van szükség. Képzeljük el, hogy mekkora munkát jelentett ezekkel a számokkal számítógép (vagy akár egyszerű számológép) nélkül számolni! Modern számítógépekkel a XX. században még nagyobb tökéletes számokat sikerült előállítani, így ma már tudjuk, hogy $2^{520}(2^{521}-1)$, $2^{616}(2^{617}-1)$, $2^{1278}(2^{1279}-1)$, $2^{2170}(2^{2171}-1)$, $2^{2202}(2^{2203}-1)$, $2^{2280}(2^{2281}-1)$, $2^{3216}(2^{3217}-1)$, $2^{44496}(2^{44497}-1)$ is tökéletes számok.[5]Ezek a számok még a mai számítógépek számára is kemény feladatot jelentenek, hiszen a fenti utolsó szám pontos leírásához majdnem 30 000 tízes számrendszerbeli számjegyre van szükség. Vajon hány tökéletes szám van még a hátralevő végtelen sok természetes szám között? Még 20, vagy 100? Egyáltalán véges számú, vagy végtelen sok? A kérdés egyszerűnek tűnik, mégis máig megfejtetlen titok.

Egy adott számról aránylag könnyű feladat eldönteni, hogy tökéletes szám-e, de mint láthattuk a tökéletes számokat megtalálni nagyon nehéz. Általánosságban is igaz, hogy ismert kulccsal a hozzá tartozó zárat kinyitni könnyű, de egy zárhoz megtalálni számtalan kulcs közül azt, amelyik kinyitja, már jóval nehezebb.

A pitagoreusok beszéltek barátságos számokról is. Azt mondták, hogy két szám barátságban áll egymással, ha bármelyikük nála kisebb pozitív osztóinak összege pontosan a másik számot adja. Barátságos számok például a 220 és 284, ugyanis

---

1 1

2 2

3 3

4 4

5 5

a 220 osztóinak összege: $1+2+4+5+10+11+20+22+44+55+110=284$,

a 284 osztóinak összege: $1+2+4+71+142=220$.

A barátságos számok története is sok évszázados történet. Már a régiek ismerték a barátságos 1184 és 1210 számpárt, majd Pierre Fermat mutatta ki ugyanezt a 17 296 és 18 416 számpárról. René Descartes (1596–1650), a matematika másik nagy alakja volt,[6]Ma már minden általános iskolás gyerek találkozik vele például a derékszögű koordinátarendszer tanulásakor, amelyet róla neveztek el Descartes-féle koordinátarendszernek. fedezte fel a barátságos 9 363 584 és 9 437 056 számpárt, majd Euler a XVIII. században még 61 barátságos számpárt talált meg.

A számmisztika már régen homályba merült, de a harmóniába, a harmonikus szépségbe vetett hit napjainkig fennmaradt. És fennmaradt az a számtalan örökérvényű gondolat, tudományos tétel is, amely e misztikus gondolkodás talaján fogant és mégis a természet mély összefüggéseit írja le. Mint a bemutatott példák is mutatják, néha olyan mély titkokat sikerült a pitagoreusoknak „számszerűsíteni", hogy még a mai napig sem ismerjük hozzájuk a kulcsot. Napjaink kriptográfiája[7]A kriptográfia a rejtjelzéssel foglalkozó tudomány. nagy részben ezekre az évezredes meg nem fejtett titkokra épül.

Igen érdekes magyar vonatkozásokra derül fény a prímszámokkal és a kis Fermat-tétellel kapcsolatban, *Kiss Elemér* marosvásárhelyi matematikus és Bolyai-kutató tollából. 1999-ben megjelent könyvében (lásd [8]) eddig ismeretlen dokumentumokra alapozva egészen új képet kapunk Bolyai Jánosról. Kiss Elemér könyvéből kiderül, hogy az idősödő Bolyai János sokat foglalkozott a prímszámokkal. Erről így ír ő maga:

„*Az egész számtan sőt az egész tan mezején alig van szebb és érdekesebb ... s a legnagyobb nyiászok (matematikusok) figyelme és eleje óta elfoglalt tárgy, mint a főszámok (prímszámok) oly mély homályban rejlő titka.*"[8]Idézet [8] 77. oldal.

Bolyai is, mint a pitagoreusok óta annyi matematikus, az úgynevezett prímszám képletet kereste, vagyis olyan formulát, amely közvetlen összefüggést ad meg az n-edik prímszám értékére. 1855 tájékán még úgy gondolta, hogy sikerült megtalálnia a titok megfejtését:

„*Azt megmutatni, hogy bármely 2^p-1 alakú szám prím mihelyt p prím, ugyanakkor amikor a $2^{2^m}+1$-gyel bajlódám, magam is megkísértettem, mert amint irataim is megmutatják én is abban a sejtelemben voltam, hogy 2^p-1 mindig prím, ha p prím. Ez egy történeti fontosságú felfedezése volna a legelső olyan függvénynek, mely mindig prímet ad. Azonban ez sem valósul meg, mert például $2^{11}-1=2047=23\cdot 89\ldots$*"[9]Idézet [8] 87. oldal.

Apja, Bolyai Farkas ösztönzésére megkísérelte bebizonyítani a kis Fermat-tétel megfordítását, mivel ha ez sikerül, akkor megkapta volna a vágyott prímszámképletet. Így például igaz-e, hogy *ha $2^{p-1}-1$ osztható p-vel, akkor p biztosan prímszám.* Néhány kísérlet után azonban rádöbbent, hogy a bizonyítás lehetetlen, a kis Fermat tétel általában nem fordítható meg. Ellenpéldákat keresve felfedezte a legkisebb úgynevezett pszeudoprím számot, a 341-et. Könnyű ellenőrizni, hogy $341=11\cdot 31$ osztója $(2^{230}-1)$-nek. Ez persze túl enyhe követelménynek tűnik, a kis Fermat-tétel minden, az n-hez relatív prím a számra megköveteli, hogy

$$a^{n-1}\equiv 1 \pmod{n} \tag{5}$$

teljesüljön. Gyorsan kiderül, hogy

$$3^{340}\equiv 56 \pmod{341},$$

így a 341 nem teljesíti a kis Fermat-tétel állításában kimondottakat.

A valódi megfordítás azt jelentené, hogy ha (5) mindannyiszor teljesül, valahányszor $(a,\ n)=1$, akkor az n prímszám. A kis Fermat-tétel azonban még így sem fordítható meg: vannak olyan összetett számok, a legkisebbik az 1729, amelyek a kis Fermat-tétel szerint prímként viselkednek.

Az ilyen n számokat nevezzük *Carmichael-számoknak,* amelyekről csak 1992-ben sikerült bebizonyítani, hogy végtelen sok létezik belőlük.

A modern kriptográfia az 1970-es években újra „felfedezte" a számelméleti eszközöket. Az időpont talán nem véletlen, hiszen ekkorra tehető a globális információs rendszerek, a globális kommunikáció, az „információ robbanás" korszakának kezdete, amely óriási feladatot jelentett az információ biztonságos tárolásával és továbbításával foglalkozóknak.

A klasszikus titkosítás megfelelő (szigorú) titoktartást és pontos szervezést igényelt, hiszen illetéktelen kezekben a „titkos kulcs" végzetes lehetett. Az *illetéktelen küldő* ugyanis képessé vált olyan üzenetek küldésére, amelyekről a fogadó nem tudhatta, hogy nem a valódi feladótól származnak, míg az *illetéktelenül a titkos kulcs birtokába jutott fogadó* el tudta olvasni a másnak címzett üzenetet. A kockázat csökkentése érdekében a titkos kulcsot rendszeresen változtatták, ami viszont igen pontos (és titkos!) szervezést igényelt, hiszen erről a változásról a küldő és fogadó fél „egyszerre" kellett, hogy értesüljön.

W. S. Jevons már 1873-ban megjelent könyvében megfogalmazta (lásd [7]) azt az elvet, hogy vannak bizonyos matematikai műveletek, amelyek elvégzése nagyon egyszerű (ilyen például az összeadás, vagy a szorzás), de az eredményből a kiindulási komponensek visszaállítása igen nehéz, sokszor reménytelen. Illusztrációként bemutatja az azóta

róla elnevezett 10 jegyű számot, a Jevons-számot (8 616 460 799), amely két prímszám szorzata, ám a prímtényezők meghatározását (a prímfaktorizációt) akkor reménytelennek látta.[10] A Jevons-szám faktorizációjára e cikk végén visszatérünk. Hogy Jevons ezzel a felvetésével mennyire megelőzte korát, azt mi sem bizonyítja jobban, mint hogy pontosan 100 év szunnyadás után, az 1970-es évek elején merült fel ismét e gondolat. Erdős Pál és Surányi János [5]-ben így fogalmazza meg a problémát:

„Létezhet-e azonban olyan rejtjelzés, amelyiknél nem lehet kitalálni, hogy hogyan kell azt visszacsinálni? Első pillanatban ez valószínűtlennek látszik, mégis az Euler–Fermat-tétel, továbbá a számítógépek rendkívüli teljesítőképessége egy oldalról, a teljesítőképességük határa a másik oldalról lehetőséget ad erre."

Világos, hogy ahhoz, hogy az Euler–Fermat-tétel alkalmazható legyen, az üzenetnek numerikusnak kell lennie, vagyis a betűkből és egyéb írásjelekből álló szövegeket számokká kell alakítani. Ez azonban könnyen megtehető a klasszikus helyettesítéses titkosítási eljárással, amikor minden egyes írásjelnek egy-egy számot feleltetünk meg.[11] Az egyik legismertebb ilyen eljárás a számítástechnikában nemzetközi szabványként alkalmazott ASCII kód, amely az ábécé kis és nagybetűihez, az elválasztó és műveleti jelekhez a 0–255 intervallum számait rendeli hozzá. Napjaink digitális világában már nem csupán a szöveges üzeneteket, hanem a kép és hang üzeneteket is számok sorozatává alakítják, így tárolják és továbbítják a kommunikációs vonalakon, aminek sok egyéb mellett az az előnye, hogy így jóval biztonságosabb adatvédelem érhető el, mint az úgynevezett analóg jeleknél. Ez azt jelenti, hogy nincs akadálya annak, hogy a továbbiakban üzeneten mindig számokat értsünk. Így már kézenfekvőbbnek tűnik, hogy a számelmélet eredményeit, ezen belül az Euler–Fermat-tételt is felhasználjuk a titkosításra. Legyen eljárásunk a következő:

a) Válasszunk két különböző p, q prímszámot, amelyek szorzata

$$pq = N. \tag{6}$$

b) Ha a továbbítandó üzenet (mint szám) nagyobb mint N, akkor bontsuk fel N-nél kisebb részekre. Egy ilyen rész legyen h. Tehát fennáll, hogy

$$0 < h < N. \tag{7}$$

c) Legyen továbbá r és m két pozitív egész szám, amelyekre

$$rm \equiv 1 \pmod{\varphi(N)}, \tag{8}$$

ami pontosan azt jelenti, hogy

$$rm = 1 + k\varphi(N), \tag{9}$$

ahol (4) szerint $\varphi(N) = (p-1)(q-1)$.

d) Ekkor az $R(h)$ rejtjelzés legyen h^r nemnegatív maradéka N-nel osztva.

e) Ha az így rejtjelzett üzenet h', akkor a megoldó kulcs $M(h')$, a $(h')^m$ nemnegatív maradéka, amely az N-nel való osztáskor keletkezik.

Be kell tehát látnunk, hogy e két kulcs kielégíti az alábbi összefüggést:

$$M(h') = M(R(h)) = h. \tag{10}$$

Nos, a fentiek szerint igazak az alábbi összefüggések:

$$M(h') = M(R(h)) \equiv h^{rm} = h^{1+k\varphi(N)} = h \cdot h^{k\varphi(N)} \pmod{N} \tag{11}$$

Ha $(h,\ N) = 1$, akkor az Euler–Fermat-tétel szerint:

$$h^{k\varphi(N)} = \left(h^{\varphi(N)}\right)^k \equiv 1 \pmod{N}. \tag{12}$$

Tehát

$$h^{rm} \equiv h \pmod{N}, \tag{13}$$

és (7) szerint (13) jobb oldala éppen h^{rm} legkisebb nemnegatív maradéka, azaz ebben az esetben teljesül a (10) összefüggés.

Vizsgáljuk most meg a még lehetséges $(h,\ N) = p$ esetet (a $(h,\ N) = q$ eset ugyanígy kezelhető). Ekkor

$$(h,\ q) = 1, \tag{14}$$

így a kis Fermat-tétel alapján

$$h^{q-1} \equiv 1 \pmod{q} \qquad \text{tehát} \qquad h^{k(p-1)(q-1)} \equiv 1 \pmod{q}. \tag{15}$$

10 10

11 11

Szorozzuk a fenti kongruenciát h-val:

$$h \cdot h^{k(p-1)(q-1)} \equiv h \pmod{hq}. \tag{16}$$

Ekkor $p \mid h$ folytán most is teljesül:

$$h^{rm} = h \cdot h^{k\varphi(N)} \equiv h \pmod{N}. \tag{17}$$

A fenti eljárás tehát kielégíti a (10) összefüggést. Ezt vették észre az 1970-es évek közepén R. L. Rivest, A. Shamir és L. Adleman az MIT (Massachusetts Institute of Technology) munkatársai, majd a részletes kidolgozás után, 1978-ban hozták nyilvánosságra (lásd [13]) és szabadalmaztatták (lásd [14]). Nevük kezdőbetűi alapján RSA algoritmusként lett közismert az egész világon és vált az egyik legnagyobb példányszámban felhasznált szoftver és hardver termékké.

Fermat 250 évvel korábbi eredményére alapozva tehát Jevons javaslata 100 évvel később megvalósult. Az RSA algoritmus valóban a titkosítás egészen új korszakát nyitotta meg, amelyet *„nyilvános kulcsú rejtjelzésnek"* hívunk. Miért?

A KöMaL szeptemberi számában (KöMaL 2001/6. 325–335. oldal) bemutatott klasszikus titkosítási eljárásokkal szemben, itt két kulccsal dolgozunk, amelyek közül az egyik nyilvánosságra hozható (ez a nyilvános kulcsnak nevezett N, r pár) anélkül, hogy a rejtjelzés biztonsága sérülne. Lássuk, miért hozható nyilvánosságra N és r.

– Jól választva két elég nagy p, q prímszámot (ezek ma már többszáz jegyű prímszámok) kiszámíthatjuk N-et és $\varphi(N) = (p-1)(q-1)$-et.

– Ezután alkalmasan választott r-rel az euklideszi algoritmust végrehajtva ellenőrizzük, hogy $(r, \varphi(N)) = 1$ teljesül-e.

– Végül r-hez meghatározzuk azt az m számot, amelyre (8) teljesül, amihez szintén euklideszi algoritmust használunk.

Mindezen műveletek közül a nagy prímszámok előállítása a legkritikusabb, de erre ma már elég gyors eljárásokkal rendelkezünk.

Ha tehát N-et és r-et mint nyilvános kulcsot közzétesszük, akárcsak a telefonkönyvben a telefonszámokat, és p, q, m-et tartjuk csupán titokban (ez utóbbi a csak általunk használható és használandó titkos kulcs), akkor ahhoz, hogy valaki illetéktelenül hozzájusson titkunkhoz, N-et kell törzstényezőkre bontania. Erről pedig érdemes felidézni Martin Gardner, a Scientific American világhírű rovatvezetőjének 1977-es gondolatait, amely éppen R. L. Rivestre hivatkozik: *„Ha a ma ismert legjobb algoritmust és a leggyorsabb számítógépeket használjuk, egy ilyen* 125*-jegyű RSA kulcs megfejtésére, Rivest becslése szerint a szükséges megfejtési idő körülbelül* 40 *kvadrillió év! Ez azt jelenti, hogy praktikusan a belátható jövőben reménytelen az RSA kulcsok faktorizáció útján történő megfejtése. Ugyanakkor maga Rivest és kollégái is elismerik, hogy semmilyen elméleti bizonyítékuk nincs arra, hogy az RSA titkosítási eljárás megfejthetetlen."*

Érdekes a gondolatok hasonlósága miatt is felidézni Jevons több mint száz évvel korábbi nézetét, amelyet a Jevons számmal kapcsolatban írt le [7]-ben:

„Meg tudja mondani az Olvasó, hogy melyik két szám összeszorzásából adódik a 8 616 460 799 *szám? Úgy gondolom, reménytelen, hogy akárki (magamat is beleértve), valaha megtudja."*

Természetesen akkor még nem voltak másodpercenként millió műveletet végző számítógépek, így a megoldás csak kézi számolással volt elképzelhető (illetve elképzelhetetlen). A technika azóta nagyot fejlődött. Ma már egy ekkora szám faktorizációja számítógéppel nem okoz problémát. Ezért használnak az RSA algoritmusnál többszáz jegyű számokat, amelyek faktorizációja a számítástechnika mai szintjén ugyanolyan reménytelennek tűnik, mint 1870-ben a Jevons számé.

Ha jól megfigyeljük, a fenti érvelésekben, amelyek a kulcs gyakorlati megfejthetetlenségéről szóltak, az elméleti érvek mellett igen *nagy szerepet kapott a technika korlátaiba vetett remény.*

Ezt a reményt (vagy reménytelenséget) azonban beárnyékolja, hogy például 1996-ban S. W. Golomb amerikai matematikus olyan egyszerű eljárást adott, amely *kézi* számolással 56 lépésben megadja a Jevons szám szorzattá bontását, és kimutatta, hogy $8\,616\,460\,799 = 96\,079 \cdot 89\,681$ (lásd [06]).

Végül a prímszámokra vonatkozó néhány egyszerű észrevételt említünk meg (bizonyítás nélkül), amelyekre építve megadható a Golomb-féle eljárás jelen szerző által javított változata, ami a Jevons-számhoz hasonlóan két, egymáshoz „közeli" prím szorzatának faktorizálására használható.

(I) *Minden* 3*-nál nagyobb* p *prímszám* $6k+1$ *vagy* $6k-1$ *alakú.*

Ha a természetes számokat az alábbi módon hat oszlopba rendezzük, (lásd 1. tábla), akkor (I) alapján az összes prímszám az 1. és az 5. oszlopban helyezkedik el; az 1. oszlopban a $6k+1$, míg az 5. oszlopban a $6k-1$ alakúak.

$6k+1$ ↓				$6k-1$ ↓	
			4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100	101	102
...					

1. tábla

(I) alapján tehát a 3-nál nagyobb prímszámok keresésekor elegendő csupán a $6k \pm 1$ alakú természetes számokat vizsgálni. Az alábbi állítás az ún. komplementer prímszita annak szükséges és elegendő feltételét adja meg, hogy egy ilyen $6k \pm 1$ alakú szám összetett legyen.

(II) *(Komplementer prímszita)*

$N = 6k+1$ akkor és csak akkor összetett szám, ha alkalmas u, $v \geq 1$ egészekkel $k = 6uv + u + v$ vagy $k = 6uv - u - v$;

$N = 6k-1$ akkor és csak akkor összetett szám, ha alkalmas u, $v \geq 1$ egészekkel $k = 6uv - u + v$ vagy $k = 6uv + u - v$

(II) következményeként megkapjuk N kéttényezős felbontását is, azaz

$N = 6k+1$ ebből $N = (6u+1)(6v+1)$ vagy $N = (6u-1)(6v-1), (18) N = 6k-1$ ebből $N = (6u+1)(6v-1$

Fontos megjegyezni, hogy mivel a komplementer prímszita nem feltételezi a $\sqrt{N}$-nél kisebb prímszámok ismeretét, így a (18), (19) felbontás megtalálására jól alkalmazható osztott (párhuzamos) algoritmus.

Most térjünk vissza a Jevons számhoz. S. W. Golomb [6] cikkében a Jevons-szám faktorizációja kapcsán bemutat egy általános eljárást a két prímtényezős szorzatok prímtényezőinek meghatározására. Ha J jelöli a szorzatot, akkor a módszer egyszerű alapötlete a következő: keressük a tényezőket $p = a + b$ és $q = a - b$ alakban, azaz próbáljuk meg a J számot két négyzetszám különbségeként előállítani:

$$J = p \cdot q = a^2 - b^2 = (a+b)(a-b), \tag{20}$$

ahol a és b természetes számok, p és q prímszámok.

A (20) összefüggéshez igen egyszerűen számolható algoritmust mutat be az a, b számok meghatározására. Az algoritmus lényeges lépései:

– Képezzük az $a_0 = [\sqrt{J}]$ kezdőértéket.

– Legyen $a_k = a_0 + k$, ahol $k = 1, 2, 3, \ldots$

– Képezzük az $a_k^2 - J$ sorozatot, amíg teljes négyzetet kapunk, azaz

$$a_k^2 - J = b_k^2. \tag{21}$$

Ekkor tehát a_k, b_k természetes számok, és így teljesül, hogy

$$J = (a_k + b_k)(a_k - b_k). \tag{22}$$

Az eljáráshoz mindössze egy memóriára van szükség, amelyben az aktuális a_k értéket tároljuk. Így akár egy zsebszámológép segítségével elvégezhetők a számítások. Igen meggyőző, hogy a Jevons által 1870-ben megoldhatatlannak tartott feladat, a $J = 8\,616\,460\,799$ szám faktorizációja, S. W. Golomb módszerével $k = 56$ lépésben célhoz vezet, és megadja az $a_{56} = 92\,880$, $b_{56} = 3199$ megoldást.[12] $a_{56}^2 - b_{56}^2 = (a_{56} - b_{56})(a_{56} + b_{56}) = \underbrace{89\,681}_{p} \cdot \underbrace{96\,079}_{q} = 8\,616\,460 = J.$

[12] 12

Más megközelítésben láttuk, hogy (II) (a komplementer prímszita) szintén megadja bármely $6k \pm 1$ alakú összetett szám kéttényezős prímfelbontását,[13](II)-ből kiderül, hogy ha J-nek két prímtényezője van, akkor mindig $6k \pm 1$ alakú. A Jevons-szám esetében például: $J = 8\,616\,460\,799 = 6 \cdot 1\,436\,076\,800 - 1$. amelynek alakja

$$J = (6u \pm 1)(6v \mp 1) \qquad (u,\ v = 1,\ 2,\ 3,\ \ldots). \tag{23}$$

Ha tehát feltételezzük, hogy J-nek két prímtényezője van (lásd (20)), akkor fennáll:

$$J = (a_k + b_k)(a_k - b_k) = (6u \pm 1)(6v \mp 1). \tag{24}$$

A két prímtényezőre vonatkozó feltétel miatt (24)-ből következik, hogy

$$a_k + b_k = 6u \pm 1, \quad \text{valamint} \quad a_k - b_k = 6v \mp 1. \tag{25}$$

A két egyenlet összeadásával adódik:

$$2a_k = 6u + 6v \Rightarrow a_k = 3(u + v). \tag{26}$$

(26)-ból következik, hogy a_k mindig osztható 3-mal. Ha tehát az a_0 kezdőértéket úgy választjuk, hogy

$$h \equiv [\sqrt{J}] \pmod 3 \Rightarrow a_0 = [\sqrt{J}] - h, \tag{27}$$

azaz a_0 osztható 3-mal, akkor a Golomb algoritmus szerint:

$$a_k = a_0 + k, \tag{28}$$

amely (27) és (28) alapján csak akkor teljesülhet, ha k is osztható 3-mal. Így a lépések számát harmadára csökkenthetjük, hiszen a $k = 1,\ 2,\ 3,\ \ldots$ lépések helyett csak a $k = 3,\ 6,\ 9,\ \ldots$ esetek vizsgálatára van szükség. A Jevons-szám esetén tehát:

$$\begin{gathered} a_0 \xrightarrow{(25)} 92823 \qquad (h = 1) \\ a_{19.3} = 92\,880, \end{gathered} \tag{29}$$

azaz 56 lépés helyett 19 lépésben előáll a megoldás. Ez az eredmény (és több másik, lásd pl. [1]) alapvetően megkérdőjelezi az RSA módszer elméleti biztonságát. A ma működő információs és kommunikációs rendszerek (internet, hálózati szoftverek, távközlési hálózatok, stb.) több mint 80%-ában RSA alapú információ-védelem van. Hogy mennyire nem alaptalan az aggodalom, azt mutatják az utóbbi 1–2 év jelentős (és sikeres) hacker támadásai, amelyeknek egy része a kulcsok megfejtésén alapult (lásd [2]).

Szeretném végül felhívni a figyelmet a matematikus és a kriptográfus gondolkodásmódbeli különbségére. Az, hogy egy adott típusú kulcsból összesen hány különböző létezik, csak akkor lenne meggyőző, ha a rejtjelfejtési támadások az úgynevezett *„teljes kipróbálás"* módszerét használnák, amelyre szinte sosem kerül sor. Ekkor lenne döntő érv az egyébként rohamosan fejlődő számítástechnikai kapacitások korlátait jellemző több évezredes és évmilliós érték.

Az érvelés ezen kívül azt is figyelmen kívül hagyja, hogy a hagyományos becslések egy-számítógépes modellekre épülnek és csak ezek sebesség és tároló kapacitását veszik figyelembe, míg a már ma is létező óriási számítógép hálózatok több száz, ezer vagy akár százezer gép kapacitását egyesítik. Ilyen internetes projektek már működnek, például a SETI program keretében, amely a földön kívüli élet kutatásával foglalkozik és a világűrből érkező óriási mennyiségű adat több százezer, internetre kapcsolt számítógépen történő osztott feldolgozásával működik. A globális hálózatok tehát egészen új technikai dimenziókat vezetnek be, amelyek szükségessé teszik azon módszerek újragondolását, amelyeknél a technikai korlátok is szerepet kapnak.

Irodalomjegyzék

[1] *Dan Boneh:* Twenty years of attack on the RSA cryptosystem. *Notices of the AMS,* February 1999, 203–213.

[2] *Dénes Tamás:* REJTJELFEJTÉS Trükkök, módszerek, megoldások. *Magyar Távközlés,* XI. évf. 4.szám, 2000. április.

[3] *T. Dénes:* Complementary Prime-Sieve *P.U.M.A.,* megjelenés alatt.

[4] *Dénes Tamás:* Titoktan, avagy kódtörő ABC (Segédeszköz és játék mellékletekkel). Kriptográfia Mindenkinek, megjelenés alatt.

[5] *Erdős Pál, Surányi János:* Válogatott fejezetek a számelméletből. *POLYGON,* Szeged, 1996.

[6] *S. W. Golomb:* On factoring Jevons' number. *CRYPTOLOGIA,* (vol. XX. no.3.) 1996.

[13] 13

[7] *W. S. Jevons:* The Principles of Science: A Treatise on Logic and Scientific Method. *Macmillan & Co., London,* 1873. Second edition 1877.

[8] *Kiss Elemér:* Matematikai kincsek Bolyai János kéziratos hagyatékából. *Typotex Kft.,* Budapest, 1999.

[9] *Sain Márton:* Nincs királyi út! (Matematikatörténet). *GONDOLAT,* Budapest, 1986.

[10] *Bruce Schechter:* Agyam nyitva áll! (Erdős Pál matematikai utazásai). *Vince Kiadó, Park Kiadó,* 1999.

[11] *Szalay Mihály:* Számelmélet. *Tankönyvkiadó,* Budapest, 1991.

[12] *W. Diffie, M. E. Hellman:* New directions in cryptography. *IEEE Trans.* 1976. IT-22.

[13] *R. L. Rivest, A. Shamir, L. Adleman:* A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM,* 1978. 21/2.

[14] *R. L. Rivest:* RSA chips (past/present/future); presented at Eurocrypt 84. Paris, France, 1984.

[15] *Jack Davies:* Pierre de Fermat (1601–1665) Mathematician and Jurist. Thesis for the Degree of Master of Philosophy, *Faculty of Arts, University of Liverpool,* 1996.

Dénes Tamás