A nyílt kulcsú titkosító algoritmus matematikai alapjait 1976-ban fektette le Ron **R**ivest, Adi **S**hamir és Len **A**dleman. A nevük kezdőbetűi alapján elnevezett RSA algoritmus napjaink egyik leggyakrabban használt adattitkosító eljárása. A szakirodalomban elérhető matematikai alapok felhasználásával magam is elkészítettem a titkosító eljárás – gyakorlatban is jól használható – programját. A kulcsgenerálás algoritmusának pontosabb vizsgálatával sikerült kimutatni, hogy a prímek mellett speciális összetett számok is kiválóan alkalmazhatók kulcsok generálásához, sőt jelentősen csökkenthetik a kulcsok előállításának időtartamát.

A dolgozat megmutatja, hogy a Fermat féle prímteszt – annak ellenére, hogy prímek keresésére nem megbízható, mert átbújhatnak rajta összetett számok is – tökéletesen alkalmas megbízható RSA kulcsok generálására.

A továbbiakban összefoglaljuk azokat a matematikai tételeket, algoritmusokat, melyek az eljárás elvi alapjait adják.

1. *Az Euler–Fermat-tétel és az Euler-féle φ függvény.*
2. *Az $ax + by = 1$ diophantoszi egyenlet megoldhatósága és a modális inverz fogalma.*
3. *A rend és a primitív gyök fogalma.*
4. *A kiterjesztett euklideszi algoritmus.*
5. *A kétkulcsos titkosítás alaptétele, kapcsolata a kétkulcsos titkosítással és az elektronikus aláírással.*
6. *Prímek keresése, tesztelése (valószínűségi becslés), „Tanúk" és „Cinkosok" viszonya.*
7. *Carmichael-számok definíciója és tulajdonságai.*
8. *A kétkulcsos titkosítás alaptételének egy fontos általánosítása (CA-tétel).*
9. *Kulcspárgenerálás összetett számokból.*

A cikkben nem bizonyított tételek igazolása megtalálható pl. Freud–Gyarmati: *Számelmélet* c. könyvében.

A következő mellékletek letölthetők a www.plwsecur.com URL címről. 1. Az a program (PLWSecur.exe), mely a fenti elvek alapján ténylegesen végre is hajtja egy adott fájl vagy mappa titkosítását, illetve annak visszafejtését – ez a program integráltan tartalmazza a kulcsgeneráló modult, de itt a CA tételt még nem alkalmazzuk. 2. Az a különálló kulcsgeneráló modul (KulcsparGen_CA.exe + Delphi source kód), mely a CA tételt már alkalmazza. A generált kulcsok természetesen tökéletesen együttműködnek a PLWSecur.exe programmal.

1. Az Euler–Fermat-tétel és az Euler-féle φ függvény

Tétel. *Ha p prím és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod{p}$ – (ez a „kis" Fermat-tétel).*

Bizonyítás. Az $a, 2a, \ldots, (p-1)a$ számokat osszuk el p-vel és a maradékok legyenek $m_1, m_2, \ldots, m_{p-1}$, azaz:

$$\begin{aligned} a &= k_1 p + m_1, \\ 2a &= k_2 p + m_2, \\ &\vdots \\ (p-1)a &= k_{p-1} p + m_{p-1}. \end{aligned}$$

A maradékok között nem lehet két egyenlő, mert ha $m_i = m_j$ lenne, akkor $(i-j)a$ osztható lenne p-vel, de ez lehetetlen, mert sem $(i-j)$, sem a nem osztható p-vel.

A fenti egyenlőségek oldalait összeszorozva $(p-1)!a^{p-1} = Kp + (p-1)!$, hiszen a jobb oldalon megjelenik a $p-1$ darab különböző maradék szorzataként $(p-1)!$. Ebből átrendezéssel következik, hogy $(p-1)!(a^{p-1}-1) = Kp$. Mivel $(p-1)!$ nem osztható p-vel, azért $a^{p-1}-1$ osztható p-vel, azaz $a^{p-1} \equiv 1 \pmod{p}$.

Definíció. Legyen $\varphi(n)$ az n-nél nem nagyobb, nemnegatív, n-hez relatív prím számok darabszáma – ez az *Euler-féle φ függvény.*

Tétel. *Ha A és N relatív prímek, akkor $A^{\varphi(N)} \equiv 1 \pmod{N}$ (Euler tétele – a kis Fermat-tétel Euler-féle általánosítása).*

A bizonyítás lényegében ugyanaz, mint a kis Fermat-tétel esetében: Legyenek $m_1, m_2, \ldots, m_{\varphi(N)}$ az N-hez relatív prím osztási maradékok, és ezek A-szorosainak is tekintsük az N-nel való osztásnál keletkező maradékait:

$$\begin{aligned} Am_1 &\equiv s_1 \pmod{N}, \\ Am_2 &\equiv s_2 \pmod{N}, \\ &\vdots \\ Am_{\varphi(N)} &\equiv s_{\varphi(N)} \pmod{N}. \end{aligned}$$

Könnyen belátható, hogy az $s_1, s_2, \ldots, s_{\varphi(N)}$ számok az $m_1, m_2, \ldots, m_{\varphi(N)}$ számok egy permutációja. Ehhez elegendő megmutatni, hogy az s_i számok relatív prímek N-hez, és nincs közöttük két egyenlő. Ha $(s_i, N) = p > 1$ lenne, akkor Am_i is osztható lenne p-vel, ami lehetetlen. Ha lenne köztük két egyenlő, akkor $A(m_i - m_j) = Am_i - Am_j$ osztható lenne N-nel, ami szintén lehetetlen, mert $(A, N) = 1$ és $|m_i - m_j| < N$. A fenti kongruenciák szorzatából – a maradékok szorzatával való egyszerűsítés után – következik az állítás.

Ha N prím, akkor $\varphi(N) = N - 1$, így belátható, hogy Euler tétele valóban a kis Fermat-tétel általánosítása.

Megemlítjük még a φ függvény néhány – későbbiekben felhasznált – alapvető tulajdonságát:

Tétel. *Ha p és q relatív prímek, akkor $\varphi(pq) = \varphi(p)\varphi(q)$.*

Speciálisan, ha p és q egymástól különböző prímek, akkor $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Tétel. *Tetszőleges $n \geq 1$ és p prím esetén $\varphi(p^n) = (p-1)p^{n-1}$.*

Bizonyítás. Mivel p prím, azért az $1, 2, 3, \ldots, p^n$ számok között p-vel csak a $p, 2p, 3p, \ldots, p^{n-1} \cdot p = p^n$ számok oszthatók, a többi relatív prím p^n-hez. A p-vel oszthatók száma p^{n-1}, tehát a fenti intervallum p^n-hez relatív prímjeinek száma $p^n - p^{n-1} = p^{n-1}(p-1)$.

Tétel. *Legyen n prímtényezős alakja*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad \textit{ahol} \quad \alpha_i > 0.$$

Ekkor $\varphi(n)$ felírható a következő szorzat alakjában:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \mid n \\ p \text{ prím}}} \left(1 - \frac{1}{p}\right).$$

2. Az $ax + by = 1$ diophantoszi egyenlet megoldhatósága és a modális inverz fogalma

Tétel. *Legyenek a és b egész számok. Az $ax + by = 1$ diophantoszi egyenletnek akkor és csak akkor van egészekből álló x, y megoldása, ha a és b relatív prímek, azaz $(a, b) = 1$.*

a) Ha a és b legnagyobb közös osztójára $(a, b) > 1$, akkor az egyenlet átírható $(a, b)(a_1 x + b_1 y) = 1$ alakba.

Semmilyen x, y pár nem elégítheti ki az előbbi egyenletet, mert a jobb oldalon álló 1 nem osztható (a, b)-vel.

b) Legyen $(a, b) = 1$. Az általánosság csorbítása nélkül feltehető, hogy a és b pozitív. Átrendezés után $x = \dfrac{1 - by}{a}$, azaz keresni kell azt az y egész számot, amelyre by-nak az a-val való osztási maradéka 1; megmutatjuk, hogy létezik ilyen y szám. A b számot szorozzuk meg az $1, 2, \ldots, a$ számokkal, és képezzük az a-val való osztás maradékait:

$$\begin{aligned} 1b &= k_1 a + m_1, \\ 2b &= k_2 a + m_2, \\ &\vdots \\ ab &= k_a a + m_a \quad (m_a = 0). \end{aligned}$$

Belátható, hogy az $m_1, m_2, \ldots, m_a$ maradékok a $0, 1, 2, \ldots, a-1$ számok egy permutációja, tehát elő kell fordulnia 1-nek is mint osztási maradéknak. Indirekte tegyük fel ugyanis, hogy van köztük két egyenlő, például $m_i = m_j$, ekkor $(i-j)b = (k_i - k_j)a$ $(\neq 0)$. Mivel $|i-j| < a$, azért $i - j$ nem lehet osztható a-val, de akkor – $(a, b) = 1$ miatt – $(i-j)b$ sem.

1. következmény. Az $ax + by = c$ diophantoszi egyenletnek mindig van megoldása, ha $(a, b) = 1$. (Ugyanis, ha x_0 és y_0 megoldása $ax + by = 1$-nek, akkor cx_0 és cy_0 megoldása $ax + by = c$-nek.)

2. következmény. Az $ax + by = (a, b)$ diophantoszi egyenletnek mindig van megoldása. Ez eredetileg *Bézout* lemmája. A megoldás nem egyértelmű, mert ha x és y megoldás, akkor $x_1 = x + kb$ és $y_1 = y - ka$ is az. Az a, b számok legnagyobb közös osztóját, illetve az egyenlet egy x, y megoldását a kiterjesztett euklideszi algoritmussal lehet meghatározni (lásd ott).

Az $ax+by = 1$ alakú diophantoszi egyenletek szoros kapcsolatban vannak az $ax \equiv 1 \pmod{n}$ alakú kongruenciákkal. Formális okok miatt az $ax \equiv 1 \pmod{n}$ kongruencia x megoldását tekinthetjük az a szám modális multiplikatív inverzének, azaz jelölhetjük így is: $x \equiv a^{-1} \pmod{n}$. Természetesen ha x_0 megoldás, akkor $x_0 + kn$ is az (k tetszőleges egész szám lehet).

Tétel. *Az* $ax \equiv 1 \pmod{n}$ *kongruenciának akkor és csak akkor van* x *megoldása, ha* $(a, n) = 1$. (*Ha van megoldás, akkor szimmetria okok miatt* $(x, n) = 1$.)

Bizonyítás. Tekintsük az $ax + ny = 1$ diophantoszi egyenletet. Ennek akkor és csak akkor van megoldása, ha $(a, n) = 1$. Másrészt, az $ax = 1 - ny$ alakból látszik, hogy az egyenlet éppen azt jelenti, hogy $ax \equiv 1 \pmod{n}$.

Következmény. Az Euler–Fermat-tételt felhasználva, ha $(a, n) = 1$, akkor az $ax \equiv 1 \pmod{n}$ kongruencia megoldása felírható $x \equiv a^{\varphi(n)-1} \pmod{n}$ alakban is. Ez az alak többnyire csak elméleti jelentőségű, mivel konkrét esetekben a modális inverz meghatározásához a kiterjesztett euklideszi algoritmust használjuk; ez eldönti, hogy az $(a, n) = 1$ feltétel teljesül-e, s ha igen, akkor egyidejűleg megadja az inverzet is.

3. A rend és a primitív gyök fogalma

Képezzük g egymás utáni $(1., 2., \ldots, k$-adik) hatványait $\bmod p$. Ha az így képzett számok között megjelenik a 0, akkor minden további szám már 0 marad. Ha nem jelenik meg a 0, akkor előbb-utóbb ciklusba esik, azaz létezik egy legkisebb $k > 1$ egész, amelyre $g \equiv g^k \pmod{p}$ lesz. Ekkor a ciklus hossza $k - 1$. (Vegyük észre, hogy ha $(g, p) = 1$, akkor 0 nem jelenik meg.)

Ha a tetszőlegesen választott g és p esetében létrejön a fenti típusú ciklus, akkor definíció szerint a ciklus hossza g *rendje* $\bmod p$ – melynek jelölése $o_p(g)$ (kiejtve ordo g $\bmod p$).

Könnyen belátható, hogy ha $(g, p) = 1$ akkor $o_p(g)$ mindig létezik, és az Euler–Fermat-tétel miatt $o_p(g) \leq \varphi(p)$. Sőt, az is belátható, hogy ha $g^k \equiv 1 \pmod{p}$, akkor a ciklikusság miatt $o_p(g)$ osztja k-t, speciálisan $o_p(g) - \varphi(p)$ is mindig fennáll.

Ha $(g, p) = 1$ és $o_p(g) = \varphi(p)$, akkor g-t p *primitív gyöknek* nevezzük $\bmod p$. Ha g primitív gyök $\bmod p$, akkor a $g^1, g^2, \ldots, g^{\varphi(p)} \equiv 1$ számok $\bmod p$ maradékai a p-hez relatív prím maradékok egy permutációját adják.

Most megmutatjuk, hogy a $(g, p) = 1$ nem csak elégséges, de szükséges feltétel is $o_p(g)$ létezésére, így arra is, hogy g primitív gyök legyen $\bmod p$. Ennek belátásához csupán azt kell észrevennünk, hogy $a \equiv b \pmod{m}$ esetén $(a, m) = (b, m)$. Ha létezik $o_p(g)$, akkor van olyan $k > 0$ egész szám, amelyre $g^k \equiv 1 \pmod{p}$, így $(g^k, p) = (1, p) = 1$, ezért $(g, p) = 1$-nek is teljesülnie kell.

Bizonyítás nélkül közöljük a primitív gyök létezésére vonatkozó alábbi tételt:

Primitív gyök pontosan (csak) az $N = 2, 4, p^k, 2p^k$ *alakú modulusokra létezik, ahol* p *páratlan prímszám és* $k > 0$ *egész.*

4. A kiterjesztett euklideszi algoritmus

Két szám legnagyobb közös osztójának meghatározására – nagy számok esetében – a prímtényezős felbontásra alapozott eljárás időben kivárhatatlan.

Az a, b számok legnagyobb közös osztóját (LNKO) a közismert euklideszi algoritmussal lehet hatékonyan meghatározni. Az eljárás kiterjesztésével (veremtechnika alkalmazásával) az $ax + by = (a, b)$ egyenlet x, y megoldását és az $ax \equiv 1 \pmod{n}$ kongruenciából az x $\bmod n$ inverzét is gyorsan kiszámíthatjuk.

Legyen M_0 és M_1 két pozitív egész szám, melyekből sorozatos maradékos osztásokkal képezzük a következő nemnegatív egészeket:

$$\begin{aligned}
M_0 &= k_0 M_1 + M_2 \quad (M_2 < M_0),\\
M_1 &= k_1 M_2 + M_3 \quad (M_3 < M_1),\\
M_2 &= k_2 M_3 + M_4,\\
&\vdots\\
M_n &= k_n M_{n+1} + 0.
\end{aligned}$$

Mivel az $M_2, M_3, \ldots$ folyamatosan csökkennek (a páros indexűek monoton csökkenek M_0-tól, míg a páratlan indexűek M_1-től lefelé), ezért az $n + 1$ osztás után a maradék 0 lesz.

Az M_{n+1} értéke (a, b), azaz az LNKO. Az, hogy M_{n+1} a kiinduló két (M_0 és M_1) szám közös osztója, következik az algoritmusból, a hátulról induló sorozatos visszahelyettesítésekből. Azt, hogy M_{n+1} a kiinduló két (M_0 és M_1) szám *legnagyobb* közös osztója a következő módon láthatjuk be: Legyen P az M_0 és M_1 számok egyik közös osztója. Az algoritmusból következik, hogy P osztója M_2-nek is, illetve tovább folytatva a gondolatmenetet valamennyi M_i-nek, beleértve M_{n+1}-et is. Tehát M_{n+1}-et osztja valamennyi P közös osztó, ezért M_{n+1} a legnagyobb közös osztó.

A fenti algoritmus hátulról visszafelé alkalmazva, lehetővé teszi az $ax + by = (a, b)$ egyenlet x, y megoldásainak meghatározását is (ez az algoritmus kiterjesztése).

Foglaljuk táblázatba a fenti algoritmus egy-egy sorának számait (A, B, R, K) az alábbiak szerint:

	A	B	$R_{(\text{maradék})}$	$K_{(\text{hányados})}$
0. lépés	M_0	M_1	M_2	k_0
1. lépés	M_1	M_2	M_3	k_1
$\vdots$				
$(n-1)$-edik lépés	M_{n-1}	M_n	M_{n+1}	k_{n-1}
n-edik lépés	M_n	M_{n+1}	0	k_n

Az A, B, R, K oszlopok számait – az i-edik sorban – jelöljük a_i, b_i, r_i, k_i-vel.

	A	B	$R_{(\text{maradék})}$	$K_{(\text{hányados})}$
0. lépés	a_0	b_0	r_0	k_0
1. lépés	a_1	b_1	r_1	k_1
$\vdots$				
$(n-1)$-edik lépés	a_{n-1}	b_{n-1}	r_{n-1}	k_{n-1}
n-edik lépés	a_n	b_n	0	k_n
$(n+1)$-edik lépés	a_{n+1}	0	$-$	$-$

Vegyük észre, hogy minden sorban az $(a_i, b_i) = a_{n+1}$ (= LNKO) azonosak minden $i = 0, \ldots, n+1$ esetén. (Az $(n+1)$-edik sort az egységes jelölés végett szúrtuk csak be.)

Az $ax + by = 1$ diophantoszi egyenlet vizsgálatánál említett 2. következmény (Bézout-lemma) miatt minden sorra igaz, hogy az $(a_i, b_i) = a_i x_i + b_i y_i$ egyenletnek van x_i, y_i megoldása. Speciálisan az $(n+1)$-edik sornál $x_{n+1} = 1$, $y_{n+1} = 0$.

Megmutatjuk, hogy az i-edik sor x_i, y_i együtthatói származtathatók az $(i+1)$-edik sor együtthatóiból, azaz hátulról visszafelé indulva az $x_{n+1}, y_{n+1} = 1, 0$ párból kiszámítható az x_0, y_0 pár, *azaz meghatározható az $(a, b) = ax + by$ diophantoszi egyenlet megoldása.*

Tegyük fel, hogy az $(a_{i+1}, b_{i+1}) = a_{i+1}x_{i+1} + b_{i+1}y_{i+1}$ egyenlet x_{i+1}, y_{i+1} megoldása már ismert. Ugyanezt az összefüggést az i-edik sorra alkalmazva $(a_i, b_i) = a_i x_i + b_i y_i$. Behelyettesítve a felfelé mutató nyilakkal jelölt egyenlőségeket, valamint felhasználva a sor elemei közötti belső összefüggést:

$$\begin{aligned}(a_i, b_i) = a_i x_i + b_i y_i = (k_i b_i + r_i)x_i + b_i y_i = (k_i a_{i+1} + b_{i+1})x_i + a_{i+1} y_i = \\ = a_{i+1}(k_i x_i + y_i) + b_{i+1} x_i = (a_{i+1}, b_{i+1}).\end{aligned}$$

Az együtthatók egyenlőségéből $x_{i+1} = k_i x_i + y_i$ és $y_{i+1} = x_i$, ahonnan átrendezéssel:

$$\begin{aligned}x_i &= y_{i+1}, \\ y_i &= x_{i+1} - k_i x_i = x_{i+1} - k_i y_{i+1},\end{aligned}$$

vagyis az i-edik sor együtthatói kiszámíthatók az $(i+1)$-edik sor együtthatóiból, tehát az eljárás végén megkapjuk a keresett x_0, y_0 megoldást.

Vegyük észre, hogy az algoritmus alkalmazásakor szükségünk van a k_i hányadosokra, melyeket az LNKO meghatározásakor veremben kell elhelyezni. Mivel az $ax \equiv 1 \pmod{n}$ kongruencia megoldása ekvivalens az $ax - ny = 1$ diophantoszi egyenlet megoldásával, a fenti eljárással az a modális inverzét is meg tudjuk határozni.

A cikk folytatása a szeptemberi számban lesz olvasható.