5. A kétkulcsos titkosítás alaptétele, kapcsolata a kétkulcsos titkosítással és az elektronikus aláírással

Tétel. *Ha p és q két különböző prímszám és az e, d pozitív egészekre $ed \equiv 1 \pmod{\varphi(pq)}$ teljesül, akkor tetszőleges m egész szám esetében igaz, hogy $m^{ed} \equiv m \pmod{pq}$.*

Bizonyítás. Az $ed \equiv 1 \pmod{\varphi(pq)}$ feltétel teljesülése konkrétan azt jelenti, hogy $ed - 1 = k(p-1)(q-1)$, ahol k pozitív egész. Azaz $m^{ed} = mm^{ed-1} = mm^{k(p-1)(q-1)} = m\left[m^{(p-1)}\right]^{k(q-1)}$.

Mivel $m^{(p-1)} \equiv 1 \pmod{p}$, ha m nem osztható p-vel, azért a fenti sorban a [...] részbe 1-et írva a következő kongruenciát kapjuk:

$$m^{ed} \equiv m \pmod{p}, \quad \text{ha} \quad (m,p) = 1.$$

Az előbbi gondolatmenetet megismételve q-ra:

$$m^{ed} \equiv m \pmod{q}, \quad \text{ha} \quad (m,q) = 1.$$

Ha tehát m nem osztható egyidejűleg sem p-vel, sem a tőle különböző q-val, akkor $m^{ed} - m$ osztható p-vel és q-val is, vagyis $m^{ed} - m$ osztható pq-val is, tehát $m^{ed} \equiv m \pmod{pq}$.

Már csak azt kell megmutatni, hogy ha m osztható p-vel vagy q-val, akkor is fennáll $m^{ed} \equiv m \pmod{pq}$. Például $m \equiv 0 \pmod{p}$ esetén hatványozással $m^{ed} \equiv 0^{ed} \equiv 0 \equiv m \pmod{p}$.

Tehát a bizonyítandó $m^{ed} \equiv m \pmod{pq}$ állítás minden m egész szám esetében fennáll.

A fenti tétel alkalmazása a kétkulcsos titkosításra, illetve elektronikus aláírásra

Kiinduláshoz rendelkezni kell két darab prímszámmal (p és q). Mivel az algoritmusban kulcsszerepet játszik az $N = pq$ szorzat, a prímeknek kellően nagyoknak kell lenni ahhoz, hogy az N szám prímtényezős felbontása ne legyen egyszerű (valós időben megoldható) feladat. (Általában p és q 500-2000 bites bináris szám).

Prímszámok kereséséhez, illetve a prímség bizonyításához alapvetően a Fermat-tételt használjuk, s ezért kiemelt jelentősége van a nagy számok (nagy hatványkitevők) hatványainak gyors kiszámolási algoritmusainak. (Az aritmetikai műveletek optimalizálásával itt nem foglalkozunk).

Prímek keresésével, illetve tesztelésével a *„Tanúk" és „Cinkosok"* részben foglalkozunk.

A kiterjesztett euklideszi algoritmussal – $N = pq$ értékéből kiindulva – viszonylag egyszerűen meghatározható egy olyan e, d számpár, mely kielégíti az alaptételben említett feltételeket. Egy tetszőlegesen választott, de $\varphi(N)$-hez relatív prím e szám-hoz kell megkeresni e modális inverzét $\bmod \varphi(N)$. Mivel esetünkben $\varphi(N) = (p-1)(q-1)$, a d inverz a kiterjesztett euklideszi algoritmussal könnyen meghatározható. Az egyedi e, d, N számhármas előállítását hívjuk kulcsgenerálásnak. A kulcsgenerálás első lépése mindig az N szám komponenseit alkotó prímek megkeresése, majd ennek függvényében az alkalmas e, d értékek kiszámolása. A kulcsgenerálást elvben mindenki – aki titkosan akar kommunikálni – elvégezheti saját számítógépes környezetében azzal a kulcsgeneráló programmal, mely az itt leírt elvek szerint dolgozik.

Az e, d, N számhármas ismeretében tetszőleges $m < N$ szám (message) átkódolható/titkosítható a $c < N$ (ciphertext) számba, illetve c visszafejthető az eredeti m-be az alábbi konvenciók betartásával:

Nevezzük az (e, N) számpárt nyilvános kulcsnak, a $(d, N = pq)$ számpárt pedig privát kulcsnak (nyilvános+privát = kulcspár). Fontos, hogy a kommunikációban résztvevők mindegyike rendelkezzen saját kulcspárral, azaz egyedi e, d, N számhármassal. Az egymás között kommunikáló partnerek saját privát kulcsukat titokban tartják, a nyilvánosat pedig – nevének megfelelően – minden kommunikációs partner számára ismertté teszik.

Legyen a küldendő szám (üzenet) m. A küldő a fogadó nyilvános kulcsával képezi a $c \equiv m^e \pmod{N}$ maradékot (message → ciphertext). A fogadó a saját privát kulcsával visszafejtheti c-ből az eredeti m-et szintén egy maradékképzéssel, mivel $c^d \equiv m^{ed} \equiv m \pmod{N}$ azaz (ciphertxt → message). Tehát a kódolt (titkosított üzenetet) kizárólag a kiválasztott fogadó partner tudja megfejteni saját privát kulcsának felhasználásával.

Ha pedig mint küldő, előbb a saját privátkulcsunkat alkalmazzuk az m üzenetre, azaz így képezzük a $c \equiv m^e \pmod{N}$ maradékot, akkor csak a kapcsolódó nyilvános kulcs tudja visszafejteni az üzenetet, vagyis aki visszafejti a nyilvános kulccsal az üzenetet (ez bárki lehet, mert a nyilvános kulcs mindenkinek elérhető) az biztos lehet abban, hogy csak a megfelelő privátkulcs tulajdonosától jöhetett az üzenet (elektronikus aláírás).

Legyen pl. p és q 1024 bites prím, akkor az $N = pq$ szám 2048 bites[1], azaz 256 byte hosszúságú szám. A fentiek szerint ezzel csak max. 256 byte-os üzenet – melyre $m < N$ is teljesül! – titkosítható. A gyakorlatban a hosszabb fájlokat blokkokra bontjuk, a titkosítás és visszafejtés is természetesen blokkonként fog történni.

Fontosnak tartom megemlíteni, hogy pl. a 256 byte hosszúságú N modulusnál csak az $m < N$ számok esetében korrekt az algoritmus. A helyes visszafejtés érdekében a PLwSecur programban ezt úgy hidaltam át, hogy a titkosításhoz az eredeti fájlt 255 byte-os blokkokra (message-ekre) bontottam, majd a keletkező max. 256 byte-os ciphertext-et 256 byte-on tároltam. Visszafejtéskor a 256 byte-os maradékból ismét 255 byte-ra lett a message redukálva.

Megjegyezzük, hogy a szükséges számítások (hatványozások és maradékos osztások) időigényessége miatt azonban nem célszerű valamennyi blokkot a fenti módon titkosítani. A gyorsítás érdekében csak az első blokkot titkosítjuk, de ez célszerűen csak azt a szimmetrikus (pl. véletlenszám) jelszót tartalmazza, mellyel a későbbi blokkokat fogjuk titkosítani, illetve a fogadó fél is ezzel a jelszóval tudja a további blokkokat visszafejteni.

[1] A cikk első része 2019. májusi számunkban jelent meg és honlapunkon is olvasható: https://www.komal.hu/cikkek/Kiss_Gabor-Az_RSA_kulcsgeneralas_es_a_Carmichael-szamok_kapcsolata_1.pdf.

[T] Ez csak akkor teljesül, ha p és q első hexadecimális jegye $\geq C$, de ez könnyen biztosítható.

6. Prímek keresése, tesztelése (valószínűségi becslés), „Tanúk" és „Cinkosok"

Az előzőekben megmutattuk, hogy a kétkulcsos titkosítás alapvetően az e, d, N számhármasokon alapul, melyekből a d és N számok nyilvánosak. A titkosítás erősségét tehát az $N = pq$ szorzat biztosítja, azaz olyan p és q prímeket kell keresni, melyek elég nagyok ahhoz, hogy a nyilvánosságra hozott szorzatuk ne legyen könnyen faktorizálható (prímtényezőkre bontható). A gyakorlatban ehhez többszáz jegyű számokat kell használni.

Jelenleg nem ismert olyan („egyszerű") képlet, amely eredményül prímszámokat adna. (A közismert $2^n - 1$ alakú számok (*Mersenne-számok*) között például vannak prímek[2], de pl. $2^{11} - 1 = 2047 = 89 \cdot 23$ nem prím.

Nagy prímszámok kiválasztása próbálgatásokkal történik, majd különböző tesztekkel általában nagy valószínűséggel kijelenthető, hogy a próbálgatással talált ún. *pszeudoprím* szám valóban prímnek tekinthető-e.

Esetünkben a prímkereséshez a próbálgatás eszköze a kis Fermat-tétel, mely szerint minden p prímre és tetszőleges a alapra – ha $(a, p) = 1$, azaz p nem többszöröse a-nak – $a^{p-1} \equiv 1 \pmod{p}$.

- Kiindulunk egy véletlenszerűen választott a alapból (célszerűen egy ismert prímszámból)
- Majd választunk egy ugyancsak tetszőleges p – de az $(a, p) = 1$ feltételnek megfelelő – páratlan számot (mely binárisan pl. 1000 bit hosszú). Természetesen p összetettségéről még nem tudható semmi.
- Összetettségi vizsgálat. Megvizsgáljuk, hogy az $a^{p-1} \equiv 1 \pmod{p}$ egyenlőség teljesül-e.

a) Ha $a^{p-1} \equiv 1 \pmod{p}$ igaz, akkor p-t pszeudóprímnek tekintjük és folytatás prímteszttel

b) Ha $a^{p-1} \equiv 1 \pmod{p}$ hamis, akkor p csak összetett szám lehet, ezért $p := p + 2$ és visszatérünk ennek a számnak az összetettségi vizsgálatára, ami $(a, p) = 1$ vizsgálatával kezdődik.

Megjegyezzük, hogy $(a, p) = 1$, illetve $a^{p-1} \equiv 1 \pmod{p}$ kiszámítására gyors algoritmusok vannak több száz jegyű számok esetére is. Az (a, p) legnagyobb közös osztó meghatározásához az euklideszi algoritmust használjuk kiterjesztés nélkül.

A tapasztalat alapján 1-2 ezer bites számok esetében általában 1000 próbálkozáson belül mindig akad néhány olyan p szám, melyre igaz az $a^{p-1} \equiv 1 \pmod{p}$ feltétel. Az így talált p számot – mely egy konkrét a alapra épül – az a alaphoz tartozó pszeudoprímnek nevezzük.

Annak eldöntéséhez, hogy egy pszeudoprím valóban prím-e további) prímtesztet kell alkalmazni. A legbiztosabb megoldás a prímtényezős felbontás lenne, de ez gyakorlatilag – időigénye miatt – végrehajthatatlan.

Az alább ismertetett eljárás (Fermat-teszt[3]) egy p szám összetettségének eldöntéséhez ismételten a kis Fermat-tételt használja, de most az a alapokat váltogatjuk. Mint látni fogjuk, a valódi prímség megállapítására az eljárás elvileg nem alkalmas, mert léteznek olyan összetett számok, melyek minden $(a, p) = 1$ a alapra – azaz univerzálisan – pszeudoprímnek bizonyulnak (*Carmichael-számok*).

Dolgozatunk fő célja annak megmutatása, hogy a Fermat-teszt mégis igen hasznos az RSA kulcsgenerálás szempontjából, mert a később ismertetendő CA-tétel miatt a valódi prímeken kívül a prímteszt „gyilkosainak" tekintett Carmichael-számok is – könnyen teljesíthető szűrési feltétellel – felhasználhatók RSA kulcspárok generálásához.

A Fermat-teszt leírásához szükségünk van a következő fogalmakra: A tesztelendő szám legyen p. Egy tetszőleges a szám, mely teljesíti az $(a, p) = 1$ és $a < p$ feltételeket lehet Tanú vagy Cinkos.

Tanú: Ha $a^{p-1} \not\equiv 1 \pmod{p}$, akkor az a szám TANÚ arra, hogy p összetett szám.

Cinkos: Ha $a^{p-1} \equiv 1 \pmod{p}$, akkor az a szám CINKOS p prímségéhez, ugyanis ebből még nem következik p prímsége, de lehet prím is.

p tanúinak száma legyen T, p cinkosainak száma pedig C, nyilvánvaló, hogy $T + C = \varphi(p)$.

Nyilván igazak a következők:

- Tetszőleges p szám esetén 1 és $p - 1$ relatív prím p-hez, továbbá mindkettő p cinkosa[4].
- Ha p prím, akkor minden $a < p$ szám – Euler tétele miatt - cinkos, azaz $T = 0$ és $C = \varphi(p)$. (*A prímek mellett az összetett Carmichael-számokra is* $T = 0$).
- Ha $T > 0$ (azaz p-nek van tanúja), akkor p csak összetett lehet.

[2] A *gyakoriság* 1 ezrelék alatti. 2016. január 7-én fedezték fel a a 49-ik Mersenne-prímet, ez a $2^{74\,207\,281} - 1$ szám, és 22 338 618 számjegyből áll. Jelenleg ez a legnagyobb ismert prímszám. (Wikipédia)

[3] Fermat-prímteszt helyett következetesen Fermat-tesztet használunk, mert a teszt eredménye a prímek mellett összetett számokat is prímnek vélelmez.

[4] $(p - 1) \equiv -1 \ (p)$, mindkét oldalt felemelve a $(p - 1)$-edik (ez páros!) hatványra belátható, hogy $p - 1$ cinkosa p-nek.

Most pedig megmutatjuk, hogy ha egy p számra $T > 0$, akkor $T \geq C$ is igaz, azaz ha egy p számnak van tanúja, akkor a p-hez relatív prím, $\varphi(p)$ darab szám legfeljebb fele lehet cinkos.

Legyen t a p szám tanúja, c pedig egyik cinkosa (cinkos mindig van!) Vegyük észre, hogy ha c a p-nek cinkosa, akkor $tc \pmod p$ tanú. ($(tc)^{p-1} = t^{p-1}c^{p-1} \equiv t^{p-1} \neq 1 \pmod p$ miatt.) Továbbá, ha c_1 és c_2 ap-nek két különböző cinkosa, akkor a belőlük származtatott tc_1 és tc_2 tanúk is különbözők. Ez indirekt úton látható be, ugyanis ha $tc_1 \equiv tc_2 \pmod p$ lenne, akkor $tc_1 - tc_2 = t(c_1 - c_2)$ osztható lenne p-vel. Mivel $(t, p) = 1$, ezért csak $c_1 - c_2$ osztható p-vel, ami lehetetlen $0 < |c_1 - c_2| < p$ miatt. Tehát a cinkosokból származtatható tanúk miatt $T \geq C$ lehet csak.

Ha $T > 0$, illetve következményként $T \geq C$, akkor a $T + C$ darab p-hez relatív prím (és p-nél kisebb) számok között a cinkosok előfordulási valószínűsége $\frac{C}{T+C} \leq \frac{C}{2C} = \frac{1}{2}$, azaz legfeljebb $\frac{1}{2}$.

E gondolatot folytatva, válasszunk véletlenszerűen pl. 100 db p-nél kisebb és p-hez relatív prím a számot – és ezek mindegyikére végezzük el az $a^{p-1} \equiv 1? \pmod p$ vizsgálatot, azonban ügyelve arra, hogy az első tanú felbukkanása után a vizsgálatot rögtön megszakítsuk és próbálkozzunk egy másik p-vel. Ha a p szám kiállta az előbbi próbát, elvben két eset lehetséges:

- p-nek nincs tanúja, azaz $T = 0$. Ebben az esetben p-nek csak *cinkosai* vannak, ezért ha p-t *univerzális pszeudóprímnek* tekintjük, garantáltan nem tévedünk.
- p-nek van tanúja, azaz $T > 0$. Ebben az esetben annak a valószínűsége, hogy a 100 vizsgált a szám mindegyike *cinkos* legyen kisebb, mint $(\frac{1}{2})^{100} \approx 10^{-30}$.

  Ha tehát ezek után p-t *univerzális pszeudóprímnek* tekintjük, a tévedés valószínűsége kisebb, mint $(\frac{1}{2})^{100} \approx 10^{-30}$.

(Az előbbi gondolatmenetben említett univerzális pszeudoprímek lehetnek valódi prímek is, de megbújhatnak köztük összetett számok is.)

1910-ben Carmichael találta meg az első olyan összett számot (561), melyre $T = 0$ és $C = \varphi(561)$. A TanúCinkos-kereső programmal azonban számos olyan olyan p *összetett* számot találhatunk, melyekre $T = 0$ és $C = \varphi(p)$. Tehát hiába minősül minden vizsgált, p-hez relatív prím cinkosnak, p mégis lehet összetett. Ezeket a p összetett számokat nevezzük univerzális pszeudóprímeknek, vagy Carmichael-számoknak.

7. Carmichael-számok definíciója és tulajdonságai

Definíció. Azokat az N összetett számokat, melyekre minden $(a, N) = 1$ feltételt kielégítő a alap esetén $a^{N-1} \equiv 1 \mod N$ teljesül, Carmichael-számoknak nevezzük.

Ilyen számok léteznek, a TanúCinkos-kereső program használatával bizonyíthatóan 43 darab ilyen szám van 1 millió alatt (lásd a számok listáját – a lista előállításának időigénye néhány perc volt). 1994 óta azt is tudhatjuk, hogy végtelen sok Carmichael-szám létezik.

Csak az arányok érzékeltetéséhez megjegyezzük, hogy az 1 *milliónál kisebb prímszámok* (1–999 983) *darabszáma* 78 498. *Ehhez jön még* 43 db *Carmichael-szám, azaz összesen* 78 541 db *szám esetében a Fermat-teszt mindig „prímet" vélelmez. Az* 1 *millió alatti prímtesztek tévedési aránya tehát* $43/78\,541 \approx 5{,}5 \cdot 10^{-4}$.

Korselt már 1899-ben kritériumot fogalmazott meg a Carmichael-számokra, bár még nem ismert egyet sem. Eszerint az N szám akkor és csak akkor Carmichael-féle, ha négyzetmentes, és N mindegyik p prímosztójára igaz, hogy $p - 1 \mid N - 1$ (azaz $p - 1$ osztja $(N - 1)$-et).

Az alábbi tételek egy Carmichael-szám jellemző tulajdonságait mondják ki:

- N prímtényezős felbontásában a 2-nél nagyobb prímtényezők 1-es kitevővel szerepelhetnek.
- Ha p az N egyik prímtényezője, akkor $p - 1 \mid N - 1$ (azaz $p - 1$ osztja $(N - 1)$-et).
- Az N szám nem lehet páros.
- Az N szám nem lehet két páratlan prímszám szorzata.

Bebizonyítjuk továbbá:

- ha az N szám különböző páratlan prímek szorzata, és minden prímtényezőjére teljesül, hogy $p - 1 \mid N - 1$, akkor N Carmichael-szám.

A továbbiakban N legyen definíció szerinti Carmichael-szám.

1. tétel. *N prímtényezős felbontásában a 2-nél nagyobb prímtényezők 1-es kitevővel szerepelhetnek.*

Indirekt módon tegyük fel, hogy $N = p^k m$ alakú, ahol p páratlan prím, $k \geq 2$ és $(m, p^k) = 1$. Legyen $g > 1$ primitív gyök $\mod p^k$ ($p = 2$ esetén ez nem lenne garantálható). Tekintsük az $X \equiv g \pmod{p^k}$ és $X \equiv 1 \pmod{m}$ kongruenciarendszert. Mivel $(m, p^k) = 1$, azért X létezik[5] és $(X, N) = 1$ is igaz. Ez utóbbi belátásához vegyük észre, hogy az első kongruencia fennállása miatt $(X, p^k) = 1$, a második kongruencia fennállása miatt – kihasználva *A rend és a primitív gyök fogalma* részben említett észrevételünket, miszerint *ha $a \equiv b \pmod{m}$, akkor* $(a, m) = (b, m) - (X, m) = (1, m) = 1$, tehát $(X, N) = (X, p^k m) = 1$ is igaz.

Az X teljesíti a következőket: A Carmichael-szám definíciója miatt $X^{N-1} \equiv 1 \pmod{N}$ – ugyanis $(X, N) = 1$, ezért $\varphi(p^k) \mid N - 1$. Itt azonban ellentmondásra jutunk, ugyanis $k \geq 2$ esetén $p \mid \varphi(p^k) = p^{k-1}(p-1) \mid N - 1$, de ez lehetetlen, mert p egyidejűleg nem lehet osztója $(N-1)$-nek és N-nek is.

2. tétel. *Ha p az N egyik prímtényezője, akkor $p - 1 \mid N - 1$.*

A $p = 2$ esetében az állítás triviálisan teljesül – bár, mint később látni fogjuk, N nem lehet páros szám. Így az egyik páratlan p prímet kiválasztva feltételezhetjük, hogy $N = pm$ alakú, ahol $(m, p) = 1$. Legyen g primitív gyök mod p. Tekintsük az $X \equiv g \pmod{p}$ és $X \equiv 1 \pmod{m}$ kongruenciarendszert. Mivel $(m, p) = 1$, létezik ilyen X, és $(X, N) = 1$.

A Carmichael-szám definíciója miatt $X^{N-1} \equiv 1 \pmod{N}$, így nyilván $X^{N-1} \equiv 1 \pmod{p}$, ezért $p - 1 = \varphi(p) = o_p(X) \mid N - 1$.

3. tétel. *Az N szám nem lehet páros.*

Legyen N egyik páratlan prímosztója p, ekkor a 2. tétel szerint $p - 1 \mid N - 1$. Itt $p - 1$ páros, így $N - 1$ is páros, tehát N páratlan.

4. tétel. *Az N szám nem lehet két páratlan prímszám szorzata.*

Indirekt módon tegyük fel, hogy $N = pq$ alakú. Mivel $p - 1 \mid N - 1$ fennáll, azért

$$\frac{pq-1}{p-1} = \frac{pq-q+q-1}{p-1} = q + \frac{q-1}{p-1}$$

is egész, tehát $\dfrac{q-1}{p-1}$ is egész szám. A $q - 1 \mid N - 1$ fennállásából pedig belátható, hogy $\dfrac{p-1}{q-1}$ is egész. A reciprokok csak akkor lehetnek egészek, ha mindkettő értéke 1, azaz $p = q$. A $p = q$ eset azonban az 1. tétel miatt nem lehetséges, tehát az N szám nem lehet két tényezős.

A továbbiakban N legyen különböző páratlan prímek szorzata, és minden p prímtényezőjére $p - 1 \mid N - 1$.

5. tétel. *Ha N eleget tesz a fenti feltételeknek, akkor N Carmichael-szám.*

Bármelyik p prímtényezőre $k = \dfrac{N-1}{p-1}$ egész szám. Ha $(a, N) = 1$, akkor erre az a alapra a kis Fermat-tétel szerint $a^{N-1} \equiv a^{k(p-1)} \equiv 1 \pmod{p}$. Mivel ez a kongruencia mindegyik p prímtényezőre fennáll, azért a modulusok szorzatára is, így $a^{N-1} \equiv 1 \pmod{N}$ is igaz.

8. A kétkulcsos titkosítás alaptételének egy fontos általánosítása (CA-tétel)

Az eredeti – korábban bebizonyított állítás – a következő: Ha p és q két különböző prímszám, és az e, d pozitív egészekre $ed \equiv 1 \mod \varphi(pq)$ teljesül, akkor tetszőleges m egész számra $m^{ed} \equiv m \pmod{pq}$.

Az általánosítás a következő:

Legyen N négyzetmentes szám – azaz egymástól különböző – $p_1, p_2, \ldots, p_n$ prímek szorzata. Ha az e, d pozitív egészekre teljesül az $ed \equiv 1 \big(\mod \varphi(N)\big)$ feltétel, akkor tetszőleges m egész számra $m^{ed} \equiv m \pmod{N}$).

Bizonyítás. Ugyanaz, mint két prím szorzatának az esetében.

Ennek az általánosításnak az a jelentősége, hogy a kulcsgeneráláshoz felhasználhatjuk a Fermat-tesztet kiállt valamennyi számot, függetlenül attól, hogy az valódi prím vagy összetett Carmichael-szám. Az N szorzat négyzetmentességének biztosításához elegendő a felhasznált számok páronkénti relatív prímsége, ami könnyen biztosítható.

Eddig még nem vizsgáltuk, hogy az $ed \equiv 1 \mod \varphi(N)$ feltétel hogyan teljesíthető. Itt $\varphi(N) = (p_1 - 1)(p_2 - 1)\ldots(p_n - 1)$. A kiterjesztett euklideszi algoritmussal – indulásként például egy kisebb prímet választva e értékének – igen gyorsan meghatározható d értéke – ha létezik megoldás. Ha nincs megoldás, akkor egy másik prím értéket választhatunk stb.

9. Kulcspárgenerálás összetett számokból

[5] Ez következik abból, hogy az $ax + by = 1$ diofantoszi egyenletnek csak akkor van megoldása, ha $(a, b) = 1$, továbbá ekkor az $ax + by = c$ diofantoszi egyenletnek is van megoldása.

A CA-tétel egyik fontos következménye, hogy az RSA kulcspárok generálását prímek mellett speciális összetett számokkal is meg lehet csinálni, mégpedig pont azokkal, melyek a Fermat-teszt prímvizsgálatát „meggyilkolták".

A PLwSecur (v2.2) változatában 256 bites, illetve 512 bites prímeket használunk, nevezetesen

– az 512 bites kulcspár 2 db 256 bites prím szorzatából,

– a 768 bites kulcspár egy 256 bites és egy 512 bites prím szorzatából,

– az 1024 bites kulcspár 2 db 512 bites prím szorzatából

van generálva.

Bár a program jelenlegi változata max. 2048 bites kulcspárokat is tud kezelni, az alkalmazott programtechnika (Delphi kód, de nincsenek beágyazott assembler gyorsítások) nem alkalmas hosszabb kulcspárok generálására észszerű időn belül.

A CA-tétel alapján azonban lehetőség nyílik 1536, 2048 bithosszúságú kulcsok generálására 512 bites prímek felhasználásával. A kulcsgenerálás folyamata a következő lehet:

1. A végcéltől függően generálni kell pl. 3-4 darab 512 bites prímet. Ezeket előbb szigorú prímtesztnek kell alávetni (pl. 100 erősségű Fermat-teszt). Mivel ez valószínűségi teszt, ezért a valódi prímeken kívül – nagy valószínűséggel – csak az összetett Carmichael-számok bizonyulhatnak „prímnek". (A *Prímek keresése, tesztelése* részben megmutattuk, hogy 100 darab sikeres „cinkostalálat" után annak valószínűsége, hogy p ne univerzális pszeudóprím legyen kisebb, mint $(\frac{1}{2})^{100} \approx 10^{-30}$.)

2. Az így talált számokat – beleértve az esetleges Carmichael számokat is – jelöljük $c_1, c_2, \ldots, c_n$-nel. A CA-tétel miatt kulcsgeneráláshoz csak akkor használhatók, ha szorzatuk négyzetmentes. Ehhez elegendő azt biztosítani, hogy a számok páronként relatív prímek legyenek. Ha valamelyiknél sérül a relatív prímség, akkor helyette másik számot kell generálni az előző pont szerint.

3. A fenti előkészítések után az $N = c_1 c_2 \ldots c_n$ szorzat értéke mellé meg kell határozni $Q = (c_1-1)(c_2-1)\ldots(c_n-1)$ értékét is, majd az $ed \equiv 1 \mod Q$ egyenletnek eleget tevő e, d, N hármasból képezhető a kulcspár. Vegyük észre, hogy a c_i számok prímtényezős felbontásában szereplő valamennyi p_j prímre fennáll, hogy $p_j - 1 \mid c_i - 1$. Ezért a CA tétel bizonyításakor az $ed \equiv 1 \mod Q$ feltétel is elegendő.

Természetesen tisztában kell lenni azzal, hogy pl. 4 darab 512 bites számból származtatott 2048 bites kulcspár kevésbé biztonságos (elméletileg könnyebben faktorizálható), mint ha ugyanezt 2 darab 1024 bites számból származtattuk volna. Ugyanakkor a kulcsgenerálás időigénye *nagyságrendekkel rövidebb* lesz. A kulcspár használatakor az encryt/decrypt időigényét az e, N (nyilvános), illetve d, N (privát) számpárok mérete határozza meg, ami már teljesen független az e, d, N számok előállításának módjától, azaz itt a futási időben változás nem várható.

Megjegyzendő végül, hogy ha a prímtesztelésnél a nagyon nagy valószínűséggel helyes eredmény helyett a biztosan jó válaszhoz ragaszkodunk, akkor immár ez az igény is kielégíthető – az algoritmus bonyolultságának növekedése árán. Mindezt Agrawal, Kayal és Saxena 2002-ben publikált eredménye biztosítja.

1 *millió alatti Carmichael-számok* (43 db)

Hex	Dec	Prímfelbontás	Hex	Dec	Prímfelbontás
231	561	$3 \cdot 11 \cdot 17$	3DAB9	252 601	$41 \cdot 61 \cdot 101$
451	1105	$5 \cdot 13 \cdot 17$	44011	278 545	$5 \cdot 17 \cdot 29 \cdot 113$
6C1	1729	$7 \cdot 13 \cdot 19$	47E09	294 409	$37 \cdot 73 \cdot 109$
9A1	2465	$5 \cdot 17 \cdot 29$	4CDC5	314 821	$13 \cdot 61 \cdot 397$
B05	2821	$7 \cdot 13 \cdot 31$	51949	334 153	$19 \cdot 43 \cdot 409$
19C9	6601	$7 \cdot 23 \cdot 41$	53251	340 561	$13 \cdot 17 \cdot 23 \cdot 67$
22CF	8911	$7 \cdot 19 \cdot 67$	61699	399 001	$31 \cdot 61 \cdot 211$
2959	10 585	$5 \cdot 29 \cdot 73$	641B9	410 041	$41 \cdot 73 \cdot 137$
3DE1	15 841	$7 \cdot 31 \cdot 73$	6DA29	449 065	$5 \cdot 19 \cdot 29 \cdot 163$
729D	29 341	$13 \cdot 37 \cdot 61$	775B1	488 881	$37 \cdot 73 \cdot 181$
A051	41 041	$7 \cdot 11 \cdot 13 \cdot 41$	7D1CD	512 461	$31 \cdot 61 \cdot 271$
B641	46 657	$13 \cdot 37 \cdot 97$	819C1	530 881	$13 \cdot 97 \cdot 421$
CD99	52 633	$7 \cdot 73 \cdot 103$	86F11	552 721	$13 \cdot 17 \cdot 41 \cdot 61$
F519	62 745	$3 \cdot 5 \cdot 47 \cdot 89$	A04D9	656 601	$3 \cdot 11 \cdot 101 \cdot 197$
F9E5	63 973	$7 \cdot 13 \cdot 19 \cdot 37$	A0D71	658 801	$11 \cdot 13 \cdot 17 \cdot 271$
12661	75 361	$11 \cdot 13 \cdot 17 \cdot 31$	A3951	670 033	$7 \cdot 13 \cdot 37 \cdot 199$
18AED	101 101	$7 \cdot 11 \cdot 13 \cdot 101$	B6C71	748 657	$7 \cdot 13 \cdot 19 \cdot 433$
1C4D1	115 921	$13 \cdot 37 \cdot 241$	C97B1	825 265	$5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
1ED09	126 217	$7 \cdot 13 \cdot 19 \cdot 73$	CCA39	838 201	$7 \cdot 13 \cdot 61 \cdot 151$
27A61	162 401	$17 \cdot 41 \cdot 233$	D0369	852 841	$11 \cdot 31 \cdot 41 \cdot 61$
2A031	172 081	$7 \cdot 13 \cdot 31 \cdot 61$	F3901	997 633	$7 \cdot 13 \cdot 19 \cdot 577$
2E02D	188 461	$7 \cdot 13 \cdot 19 \cdot 109$			