6. fejezet

Számelmélet és rejtjelezési eljárások

Számelméleti alapok. RSA és alkalmazásai, Diffie-Hellman-Merkle kulcscsere.

6.1. Halmazelméleti alapfogalmak

6.1.1. Definíció (Részbenrendezés, rendezés, jólrendezés). *Egy X halmazbeli reláció részbenrendezés, ha tranzitív, reflexív és antiszimmetrikus.*

A részbenrendezés teljes rendezés (röviden rendezés), ha dichotom (azaz bármely két elem összehasonlítható).

Az X részbenrendezett halmaz jólrendezett, ha X bármely nem üres részhalmazának van legkisebb eleme.

6.1.2. Definíció (Ekvivalenciareláció). *Egy relációt ekvivalenciarelációnak nevezünk, ha reflexív, szimmetrikus és tranzitív.*

6.1.3. Definíció (Osztályozás kompatibilitása művelettel (relációval)). *Legyen X halmaz, $*$ binér művelettel (relációval). Legyen adott X egy osztályozása (a hozzá tartozó ekvivalenciareláció legyen $\sim$). Azt mondjuk, hogy $*$ kompatibilis az osztályozással, ha $x \sim x'$ és $y \sim y'$ esetén $x * y \sim x' * y'$ ($x \sim x'$ és $y \sim y'$ esetén $x * y$-ból következik $x' * y'$).*

6.2. Csoportelméleti alapfogalmak

6.2.1. Definíció (Félcsoport). *Ha $*$ művelet a G halmazon asszociatív, akkor a $(G, *)$ párt félcsoportnak nevezzük.*

6.2.2. Definíció (Semleges elem). *Egy G halmaz s eleme bal, illetve jobb oldali semleges elem, ha $\forall g \in G : s * g = g$, illetve $g * s = g$. s semleges elem, ha bal és jobb oldali semleges elem.*

6.2.3. Definíció (Inverz). *Ha a G félcsoportban van semleges elem, és $g, g^* \in G$-re $g * g^* = s$, akkor g^* a g-nek jobbinverze, illetve g a g^*-nak balinverze. Ha g^* a g-nek balinverze és jobbinverze, akkor inverze.*

6.2.4. Definíció (Csoport). *Ha egy semleges elemes félcsoport minden elemének van inverze, akkor csoportnak nevezzük.*

6.2.5. Definíció (Kommutativitás). *A $*$ művelet a G halmazon kommutatív, ha $\forall f, g \in G : f * g = g * f$.*

6.2.6. Definíció (Abel-csoport). *A kommutatív csoportokat Abel-csoportnak nevezzük.*

6.2.7. Definíció (Gyűrű). *Egy R halmazt a $(+, \cdot)$ binér műveletekkel gyűrűnek hívunk, ha az összeadással Abel-csoportot, a szorzással félcsoport, teljesül a mindkét oldali disztributivitás.*

6.2.8. Definíció (Nullosztó). *Ha R gyűrű x, y nullától különböző elemeire $xy = 0$, akkor őket nullosztópárnak nevezzük, ahol x bal oldali, y jobb oldali nullosztó.*

Egy legalább kételemű gyűrűt nullosztómentesnek nevezünk, ha nincsenek benne nullosztópárok.

6.2.9. Definíció (Integritási tartomány). *Kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezünk. Rendezett integritási tartományról beszélünk, ha rendezett halmaz, integritási tartomány és az összeadás, valamint a szorzás monoton.*

6.2.10. Tétel (Integritási tartomány és a szigorú monotonitás). *Egy rendezett halmaz, mely integritási tartomány, pontosan akkor rendezett integritási tartomány, ha az összeadás és a szorzás* szigorúan *monoton.*

6.2.11. Definíció (Ferdetest, test, rendezett test). *Egy F gyűrűt ferdetestnek nevezünk, ha a nullelemet 0-val jelölve $F \setminus \{0\}$ a szorzással csoport.*

Ha a szorzás kommutatív is, akkor F-et testnek nevezzük.

Test rendezett test, ha test és rendezett integritási tartomány.

6.2.12. Definíció (Felső határ tulajdonság). *Egy rendezett testet felső határ tulajdonságúnak hívunk, ha minden nem üres, felülről korlátos részhalmazának van legkisebb felső korlátja.*

6.2.13. Definíció (Archimédeszi tulajdonság). *Egy F rendezett testet archimédeszi tulajdonságúnak nevezünk, ha $x, y \in F$, $x > 0$ esetén van olyan $n \in \mathbb{N}$, melyre $nx \geq y$.*

6.3. A számelmélet alapjai

6.3.1. A természetes számok

A természetes számok definiálására a Peano-féle axiómarendszert használjuk. Megjegyzendő, hogy az axiómarendszer (bizonyos értelemben) egyértelműen meghatározza a természetes számok halmazát, azonban bármelyik axiómát elhagyva az egyértelműség nem teljesül.

6.3.1. Definíció (Peano-axiómák).

1. $0 \in \mathbb{N}$,
2. *ha* $n \in \mathbb{N}$, *akkor* $n^+ \in \mathbb{N}$,
3. *ha* $n \in \mathbb{N}$, *akkor* $n^+ \neq 0$,
4. *ha* $n, m \in \mathbb{N}$ *és* $n^+ = m^+$, *akkor* $n = m$,
5. *ha* $S \subset \mathbb{N}$, $0 \in S$ *és ha* $n \in S$, *akkor* $n^+ \in S$, *akkor* $S = \mathbb{N}$.

6.3.2. Tétel (A természetes számok létezése). *Van olyan* $(\mathbb{N}, (0,^+))$ *pár, amely eleget tesz Peano axiómáinak.*

A bizonyítás során belátjuk, hogy egy ω halmaz az $\emptyset$-zal mint nullával és a $^+ : x \mapsto x \cup \{x\}$ művelettel elget tesz a Peano-axiómáknak.

6.3.3. Tétel (A természetes számok egyértelműsége). *Bármely két, a Peano-axiómáknak eleget tevő halmaz között létezik olyan kölcsönösen egyértelmű φ leképezés, melyre $\varphi(0) = 0$ és $\varphi(n^+) = \varphi(n)^+$.*

A bizonyítás a rekurziótétel és az ötödik Peano-axióma segítségével történik.

6.3.4. Tétel (Rekurziótétel). *Legyen X egy halmaz, $a \in X$ és $f : X \to X$ függvény. Ha a Peano-axiómák teljesülnek, akkor egy és csak egy olyan $g : \mathbb{N} \to X$ függvény létezik, melyre $g(0) = a$ és $g(n^+) = f(g(n))$.*

Ismeretes az általános rekurziótétel fogalma is, ld. pl. Járai Antal: Bevezetés a matematikába *c. jegyzetét.*

6.3.5. Definíció (Karakterisztikus függvény). *Legyen X halmaz, $Y \subset X$, $\delta(x) = 1$ ha $x \in Y$ és $\delta(x) = 0$, ha $x \in X \backslash Y$. A δ függvényt az Y halmaz X-re vonatkozó karakterisztikus függvényének nevezzük.*

6.3.2. Műveletek természetes számokkal

6.3.6. Definíció (Összeadás és szorzás). *A rekurziótétel alapján minden m természetes számhoz létezik $s_m : \mathbb{N} \to \mathbb{N}$, hogy $s_m(0) = m$ és $\forall n \in \mathbb{N} : s_m(n^+) = (s_m(n))^+$. Az $s_m(n)$ számot jelöljük $m + n$-nel, és nevezzük az m és n számok összegének!*

A rekurziótétel alapján minden m természetes számhoz létezik $p_m : \mathbb{N} \to \mathbb{N}$ függvény, melyre $p_m(0) = 0$ és $\forall n \in \mathbb{N} p_m(n^+) = (p_m(n)) + m$. A $p_m(n)$ számot jelölje $m \cdot n$ és nevezzük az m és n szorzatának!

6.3.7. Tétel (Az összeadás és a szorzás tulajdonságai).
Ha $k, m, n \in \mathbb{N}$

1. *$(k + m) + n = k + (m + n)$ (asszociativitás),*
2. *$0 + n = n + 0 = n$ (0 a nullelem),*
3. *$m + n = n + m$ (kommutativitás),*
4. *ha $m + k = n + k$, akkor $m = n$ (egyszerűsítési szabály);*

illetve

1. *$(k \cdot m) \cdot n = k \cdot (m \cdot n)$ (asszociativitás),*
2. *$0 \cdot n = n \cdot 0 = 0$ (a 0 a nullelem),*
3. *$1 \cdot n = n \cdot 1 = n$ (az 1 az egységelem),*
4. *$m \cdot n = n \cdot m$ (kommutativitás),*
5. *$k \cdot (m + n) = k \cdot m + k \cdot m$ (disztributivitás).*

6.3.8. Tétel (A természetes számok helye a csoportelméletben). *A természetes számok mind az összeadással, mind a szorzással kommutatív félcsoport. Az összeadás nulleleme a* 0*, illetve a szorzás egységeleme az* 1*.*

6.3.9. Tétel (A természetes számok rendezése). *Legyen* $m, n \in \mathbb{N}$ *esetén* $m \leq n$*, ha* $\exists k \in \mathbb{N}$*, hogy* $m + k = n$*. A természetes számok halmaza a* $\leq$ *relációval jólrendezett (azaz rendezett is).*

6.3.10. Tétel (A maradékos osztás tétele). *Legyen* $n > 0$ *természetes szám. Minden* m *természetes szám egyértelműen felírható* $m = q \cdot n + r$ *alakban, ahol* $q, r \in \mathbb{N}$ *és* $r < n$*.*

6.3.3. Egész számok

6.3.11. Definíció (Egész számok). *Tekintsük az* $\mathbb{N} \times \mathbb{N}$ *halmazt, ahol*

- $(m, n) \sim (m', n')$, *ha* $m + n' = m' + n$ *reláció,*
- $(m, n) + (m', n') = (m + m', n + n')$ *az összeadás,*
- $(m, n) \cdot (m', n') = (m \cdot m' + n \cdot n', m \cdot n' + m' \cdot n)$ *a szorzás,*
- $(m, n) \leq (m', n')$, *ha* $m + n' \leq m' + n$ *rendezés.*

Egész számoknak nevezzük a feti reláció által meghatározott ekvivalenciaosztályokat.

6.3.12. Tétel (Az egész számok tulajdonságai).

1. *a* $\sim$ *reláció ekvivalenciareláció,*
2. *az összeadás, a szorzás és a* $\leq$ *reláció kompatibilis az ekvivalenciarelációval,*
3. *a* $\leq$ *rendezés,*
4. $\mathbb{Z}$ *az összeadásra nézve Abel-csoport,*
5. $\mathbb{Z}$ *a szorzással kommutatív egységelemes félcsoport,*
6. *ha* $x \neq 0$ *és* $y \neq 0$*, akkor* $x \cdot y \neq 0$*,*
7. *a szorzás az összeadásra nézve disztributív,*

8. *az összeadás és a szorzás monoton a rendezésre.*

6.3.13. Tétel. *A természetes számok beágyazhatók az egész számok halmazába az* $n \mapsto \widetilde{(n,0)}$ *megfeleltetéssel.*

6.3.14. Tétel (Az egész számok a csoportelméletben). *Az egész számok halmaza az összeadással és a szorzással, valamint a rendezéssel egységelemes, rendezett integritási tartományt alkot.*

6.3.15. Tétel (Az általános disztributivitás tétele).

1. *ha* $m, n \in \mathbb{N}$, *és* $a_1, \ldots, a_m$ *és* $b_1, \ldots, b_n$ *egy gyűrű tetszőleges elemei, akkor*
$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$$

2. *ha* $m \in \mathbb{N}^+$, $n_1, \ldots, n_m \in \mathbb{N}$, $a_{i,j_i} \in R$, *ha* $a \leq i \leq m$, $q \leq j_i \leq n_i$, *akkor*
$$\prod_{i=1}^{m}\left(\sum_{j_i=1}^{n_i} a_{i,j_i}\right) = \sum_{j_1=1}^{n_1}\cdots\sum_{j_m=1}^{n_m}\prod_{i=1}^{m} a_{i,j_i}.$$

6.3.4. Racionális számok

6.3.16. Definíció (Racionális számok). *Tekintsük a* $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ *halmazon a következőket:*

- $(m,n) \sim (m',n')$, *ha* $mn' = nm'$ *reláció,*
- $(m,n) + (m',n') = (mn' + nm', nn')$ *összeadás,*
- $(m,n) \cdot (m',n') = (m \cdot m', n \cdot n')$ *szorzás,*
- $(m,n) \leq (m',n')$, *ha* $(m'n - n'm)nn' \geq 0$ *rendezés.*

Jelölje az $\sim$ *szerinti ekvivalenciaosztályok halmazát* $\mathbb{Q}$, *és nevezzük ezt a racionális számok halmazának.*

6.3.17. Tétel (A racionális számok tulajdonságai).

1. *a* $\sim$ *reláció ekvivalenciareláció,*

2. *az összeadás, a szorzás és a rendezés kompatibilis $\sim$-val,*

3. $\mathbb{Q}$ *az összeadással és a szorzással egységelemes integritási tartomány,*

4. $\mathbb{Q}$ *nem nula elemei a szorzással Abel-csoportot alkotnak,*

5. *az összeadás és a szorzás monoton.*

6.3.18. Tétel (Az egész számok beágyazása a racionális számok halmazába). $\mathbb{Z}$ *beágyazható* $\mathbb{Q}$*-ba az* $n \mapsto \widetilde{(n,1)}$ *leképezéssel.*

6.3.19. Tétel (A racionális számok helye a csoportelméletben). *A racionális számok az összeadással, a szorzással és a rendezéssel rendezett testet alkotnak. A racionális számok halmaza archimédeszi tulajdonságú, de nem felső határ tulajdonságú.*

6.3.5. Valós számok

6.3.20. Definíció (Valós számok). *Egy felső határ tulajdonságú rendezett testet a valós számok testének nevezünk.*

6.3.21. Tétel. *Létezik felső határ tulajdonságú test, és két felső határ tulajdonságú test között mindig van kölcsönösen egyértelmű, monoton növekedő, összeadás- és szorzástartó leképezés.*

6.3.6. Komplex számok

6.3.22. Definíció (Komplex számok). *A komplex számok halmaza* $\mathbb{C} = \mathbb{R} \times \mathbb{R}$*az alábbiakkal:*

- $(x, y) + (x', y') = (x + x', y + y')$ *összeadással és a*
- $(x, y) \cdot (x', y') = (xx' - y'y, y'x + yx')$ *szorzással.*

6.3.23. Tétel (A komplex számok tulajdonságai).

- $\mathbb{C}$ *test a fenti műveletekkel,*
- *a nullelem a* $(0, 0)$ *pár,*
- (x, y) *additív inverze a* $(-x, -y)$ *pár,*

- *az egységelem az* $(1,0)$ *pár,*
- *a nullelemtől különböző* (x,y) *elem multiplikatív inverze az* $(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2})$ *pár.*

6.3.24. Tétel (A valós számok beágyazása a komplex számok halmazába). *A valós számok beágyazható a komplex számok halmazába az* $x \mapsto (x,0)$ *megfeleltetéssel.*

6.4. Számelméleti alapok

6.4.1. Oszthatóság

6.4.1. Definíció (Oszthatóság a természetes számok körében). *Az* m *természetes számot az* n *osztójának (*n*-et pedig* m *többszörösének) nevezzük, ha* $\exists k \in \mathbb{N}$*, melyre* $m \cdot k = n$*. Jelölése* $m|n$*.*

6.4.2. Tétel (Az osztás egyértelműsége). *Az* $m = 0$ *esetet kivéve az egyszerűsítési szabály miatt legfeljebb egy, a fenti definícióban* k*-val jelölt szám létezik adott* m,n *számokhoz.*

6.4.3. Tétel (Az oszthatóság tulajdonságai a természetes számok körében).

1. *Ha* $m|n$ *és* $m'|n'$*, akkor* $mm'|nn'$*,*
2. *a nullának minden természetes szám osztója,*
3. *a nulla csak saját magának osztója,*
4. *az* 1 *minden természetes számnak osztója,*
5. *ha* $m|n$*, akkor* $\forall k \in \mathbb{N} : mk|nk$*,*
6. *ha* $k \in \mathbb{N}^+$ *és* $mk|nk$*, akkor* $m|n$*,*
7. *ha* $m|n_i$ *és* $k_i \in \mathbb{N} (i = 1, 2, \ldots, j)$*, akkor* $m|\sum_{i=1}^{j} k_i n_i$*,*
8. *bármely nem nulla természetes szám bármely osztója kisebb vagy egyenlő a számnál,*

9. *az „osztója" reláció reflexív, tranzitív és antiszimmetrikus, azaz részbenrendezés.*

6.4.4. Megjegyzés. *Az oszthatóság fogalma analóg módon megfogalmazható egységelemes integritási tartományra is. Az előző tételben felsorolt tulajdonságok igazak a 9. pont kivételével: az „osztója" reláció ugyanis ekkor csak reflexív és tranzitív, de nem antiszimmetrikus.*

6.4.5. Definíció (Törzsszámok és prímszámok). *Ha egy $n > 1$ természetes szám nem csak a triviális $n \cdot 1$ alakban írható fel szorzatként, akkor n-et* törzsszám*nak nevezzük.*

A $p > 1$ természetes szám prímszám*, ha $p|km(k, m \in \mathbb{N}$ esetén $|k$ vagy $p|m$.*

6.4.6. Megjegyzés. *Minden prímszám törzsszám. A természetes számok körében megmutatható a fordított állítás is (minden törzsszám prímszám).*

6.4.7. Tétel (A számelmélet alaptétele). *Minden természetes szám a sorrendtől eltekintve egyértelműen felírható prímszámok szorzataként.*

6.4.8. Definíció (Asszociáltak). *Ha egy R integritási tartományban $a|b$ és $b|a$, akkor azt mondjuk, hogy a és b asszociáltak. Ez a reláció ekvivalenciareláció, és az $|$ reláció kompatibilis vele, továbbá az ekvivalenciaosztályokon részbenrendezést ad.*

6.4.9. Definíció (Egységek). *Egységelemes integritás tartomány egysége olyan elem, amelynek van multiplikatív inverze.*

6.4.10. Megjegyzés. *Az egységek a szorzásra nézve Abel-csoportot alkotnak, amit az integritási tartomány* egységcsoport*jának nevezünk. Az egységek R minden elemének osztói, és ha egy elem minden elemnek osztója,akkor egység.*

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

6.4.11. Megjegyzés. *A felbonthatatlan elemek és prímelemek definíciója egységelemes integritási tartományban analóg a természetes számoknál szereplővel azzal a módosítással, hogy $a > 1$ helyett a kikötés az, hogy a nem 0 és nem egység.*

6.4.12. Definíció. (Legnagyobb közös osztó, legkisebb közös többszörös, relatív prímek). *Legyenek R egységelemes integritási tartományban $a_1, a_2, \ldots, a_n \in R, b \in R$. Ekkor*

- *b legnagyobb közös osztó, ha minden i-re $b|a_i$ és ha $b'|a_i$, akkor $b'|b$ (megj.: ha van legnagyobb közös osztó, akkor azok egymás asszociáltjai),*
- *b legkisebb közös többszörös, ha minden i-re $a_i|b$ és ha $a_i|b'$, akkor $b|b'$ (megj.: ha van legkisebb közös többszörös, akkor azok egymás asszociáltjai),*
- *ha a legnagyobb közös osztó egység, akkor az $a_1, a_2, \ldots, a_n$ elemeket relatív prímeknek nevezzük.*

6.4.13. Megjegyzés (Oszthatóság az egész számok körében). *Az egész számok körében $m|n$ pontosan akkor teljesül, ha $|m|||n|$. $\mathbb{Z}$-ben az 1 és -1 az egységek.*

6.4.14. Tétel (Bővített euklideszi algoritmus). *Az algoritmus meghatározza két egész szám (a és b) egy d legnagyobb közös osztóját, valamint x és y egészeket úgy, hogy $d = ax + by$ teljesüljön.*

1. $n, x_0, y_0, r_0, x_1, y_1, r_1 := 0, 1, 0, a, 0, 1, b,$
2. *Ha $r_{n+1} = 0$, akkor $x, y, d := x_n, y_n, r_n$, és az eljárásnak vége,*
3. $n := n + 1$, $q := \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor$,
   $r_{n+2} := r_n - r_{n+1}q_{n+1} (= r_n \bmod r_{n+1})$,
   $x_{n+2} := x_n - x_{n+1}q_{n+1}$,
   $x_{n+2} := y_n - y_{n+1}q_{n+1}$.

6.4.15. Tétel (Eukleidész tétele). *Végtelen sok prímszám van (a bizonyítás indirekt).*

6.4.16. Tétel.

- *Tetszőleges $a, b \in \mathbb{Z}$ számoknak van legkisebb közös többszöröse, illetve $lnko(a, b) \cdot lkkt(a, b) = |ab|$,*
- *$lkkt(ac, bc) = c \cdot lkkt(a, b)$.*

6.4.2. Kongruenciák

6.4.17. Definíció. *Azt mondjuk, hogy* $a \equiv b \pmod{m}$, *ha* $m|a - b$.

6.4.18. Definíció (Maradékosztályok). *Mivel a kongruencia ekvivalenciareláció* $\mathbb{Z}$*-ben, képezhetjük* $\mathbb{Z}$*nek egy adott* m *modulusú kongruencia szerinti ekvivalenciaosztályait – ezeket maradékosztályoknak nevezzük.*

6.4.19. Megjegyzés (Maradékosztályok). *Gyakori jelölés, hogy ha* a *az ekvivalenciaosztály egy reprezentánsa, akkor az ekvivalenciaosztályt* $\bar{a}$*-sal jelöljük. A maradékosztályok kompatibilisek az összeadással és a szorzással, így az* m *modulus szerinti ekvivalenciaosztályok kommutatív egységelemes gyűrűt alkotnak a műveletekkel, amelyet* $\mathbb{Z}_m$ *jelöl.*

6.4.20. Tétel. *Ha* $lnko(a, m) = 1$, *akkor a maradékosztályának van multiplikatív inverze* $\mathbb{Z}_m$*-ben. Speciálisan, ha* m *prímszám, akkor* $\mathbb{Z}_m$ *test.*

6.4.21. Definíció (Maradékosztály elemének rendje). *Legyen* $g \in \mathbb{Z}_m$, *és legyenek* $g^1, g^2, g^3, \ldots, g^k$ *különböző elemei* $\mathbb{Z}_m$*-nek,* $g^{k+1} = g$. *Ekkorazt mondjuk, hogy* k *a* g *rendje modulo* m.

6.4.22. Definíció (Primitív gyökök). *Ha* $n > 1$ *természetes szám, akkor* g *primitív gyök modulo* n, *ha* g *rendje modulo* n *pontosan* $\varphi(n)$, *ahol* $\varphi(n)$ *az Euler-féle függvényt jelöli (ld. a következő definíciót).*

6.4.23. Definíció (Euler-függvény). *Ha* $m > 0$ *egész szám, akkor jelölje* $\varphi(m)$ *az* m*-nél kisebb, vele relatív prím természetes számok számát – ez az Euler-függvény.*

6.4.24. Definíció (Lineáris kongruenciák). *Legyen* $m > 1$ *egész szám,* $a, b \in \mathbb{Z}$ *adottak. Ekkor az* $ax \equiv b \pmod{m}$ *egy lineáris kongruencia probléma.*

6.4.25. Definíció (Diofantikus problémák). *Ha egy egyenlet vagy egyenletrendszer egész megoldásait keressük, akkor* diofantikus problémá*ról beszélünk.*

6.4.26. Tétel (Kínai maradéktétel).
Legyenek $m_1, m_2, \ldots, m_n$ *egynél nagyobb, páronként relatív prím természetes számok,* $c_1, c_2, \ldots, c_n \in \mathbb{Z}$. *Az* $x \equiv c_j \pmod{m_j}$, $j = 1, 2, \ldots, n$ *kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo* $\prod_{j=1}^{n} m_j$.

6.5. Az RSA-eljárás

Az RSA rejtjelezési eljárás Rivest, Shamir és Adleman nevéhez kötődik.

Keressünk két nagy p, q prímet, és legyen $n = pq$! Válasszunk továbbá egy véletlen $1 < e < (p-1)(q-1)$ exponenst, és a bővített euklideszi algoritmussal oldjuk meg az

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

kongruenciát. (Ha azt találjuk, hogy $lnko(e, (p-1)(q-1)) > 1$, akkor keressünk új alapszámokat!)

Ha $1 < m < n$ az üzenet, akkor legyen a rejtjelezett forma $c = m^e \bmod n$. A visszafejtés módja:

$$(m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{p-1}\right)^{k(q-1)} \cdot m \equiv m \pmod{p},$$

innen a kínai maradéktétellel

$$m = c^d \bmod n.$$

Az RSA *nyilvános kulcs*a ekkor az (n, e) pár, *titkos kulcs*a a (n, d).

6.5.1. Megjegyzés (Biztonság). *Az eljárás biztonsága azon múlik, hogy n prímtényezőinek megtalálása megfelelően nagy prímek esetén emberileg beláthatatlan időt vesz igénybe.*

6.5.2. Megjegyzés (Hatékonyságnövelés). *A hatékonyság érdekében a hatványozáshoz valamilyen gyors hatványozási eljárást használhatunk, míg a megfelelően nagy prímek megkereséséhez alkalmas lehet például a* Miller-Rabin-féle valószínűségi prímteszt.

6.5.1. Az RSA felhasználásai

Titkos kommunikáció

Legyenek a kommunikáció szereplői A és B. Ekkor pl. A elkészítheti a saját kulcspárját, és a nyilvános kulcsot elküldheti B-nek. Ha B üzenetet akar küldeni A-nak, kiszámítja a $c = m^e \pmod{n}$ kódot, és ezt küldi el. A az üzenetet d birtokában már könnyen visszafejtheti.

Digitális aláírás

Tegyük fel, A biztosítani akarja az üzenetküldés folyamán B-t arról, hogy ő valóban A. Ehhez A kiszámítja az üzenetből képzett h hash-értékre az $s = h^d \bmod n$ értéket, és ezt csatolja aláírásként m-hez. Mikor B megkapja az üzenetet, az aláírást ellenőrizheti úgy, hogy A nyilvános kulcsát használva kiszámítja a hash-értéket ($h = s^e \bmod n$), majd ezt összehasonlítja az üzenetből általa képzett hash-kóddal. Ha a két kód megegyezik, akkor az üzenet valóban A-tól származik.

Diffie-Hellman-Merkle kulccsere

A DHM kulcscsere-eljárás lényege, hogy az RSA-nál gyorsabban kezelhető, szimmetrikus titkosítási eljárások kulcsai cserélhetők ki RSA segítségével nem biztonságos csatornán.

Az eljárás menete a következő (A és B szereplőkkel):

1. A és B nyilvánosan megosztanak egymással egy p prímszámot, illetve egy g generátort, hogy $g > p$ és g primitív gyök p-re nézve.
2. A és B egmyástól függetlenül generálnak egy x_A, illetve x_B véletlenszámot,
3. A és B nyilvánosan kicserélik az $y_A = g^{(x_A)} \bmod p$, illetve $y_B = g^{(x_B)} \bmod p$ értékeket.
4. ezekből az információkból a titkos kulcsot mindketten kinyerhetik az $s = y_B^{(x_A)} \bmod p = y_A^{(x_B)} \bmod p$ képlettel.

A protokoll kettőnél több résztvevőre is kiterjeszthető.