Számelmélet, csoportelmélet és titkosírás

2018. október 20.

1. Számelméleti alapok

Ebben a szakaszban néhány számelméleti alapfogalmat ismétlünk át, amelyek később a csoportelméletben és titkosírási alkalmazásokban is visszaköszönnek.

1.1. Az euklideszi algoritmus

Legyenek adottak az $a, b \in \mathbb{N}$ számok, amelyeknek a legnagyobb közös osztóját keressük. Ennek jele: (a, b). Az euklideszi algoritmus, amely megadja a legnagyobb közös osztót, a következő lépésekből áll:

1. Elosztjuk a-t b-vel, vesszük a maradékot (r_1).
2. Elosztjuk b-t r_1-gyel, vesszük a maradékot (r_2).
3. Elosztjuk r_1-et r_2-vel, vesszük a maradékot (r_3).
4. Elosztjuk r_2-et r_3-mal, vesszük a maradékot (r_4).
5. ...
6. Az eljárást addig ismételjük, amíg $r_n = 0$-t el nem érjük. A legnagyobb közös osztó az utolsó nem 0 maradék (r_{n-1}).

1.1. Példa. Mi a legnagyobb közös osztója a 186 és 42 számoknak?

Megoldás. Az euklideszi sorozat a következőképpen néz ki:

$$\begin{aligned} a &= 186, \\ b &= 42, \\ r_1 &= 18, \\ r_2 &= 6, \\ r_3 &= 0, \end{aligned}$$

tehát a legnagyobb közös osztó a 6. □

1.1. Kód. Az euklideszi algoritmus Pythonban:

```python
def euk(a,b):
    while b>0:
        a,b = b,a%b
    return a
```

Megjegyzés. Egyelőre nem világos, hogy miért is működik az euklideszi algoritmus. A következő részben ezt fogjuk megvizsgálni. Figyeljük meg alaposan a bizonyítások „logikáját” (hogyan épül fel, miből mit bizonyítunk)! Lényegében a *teljes indukció* módszerét fogjuk alkalmazni.

1.1. Állítás. *Az euklideszi algoritmus valóban egy közös osztót ad meg.*

Bizonyítás. Ismert, hogy a maradékos osztás művelete az $a, b \in \mathbb{N}$, $a \geq b$ számokra a következőképpen írható fel:

$$a = b \cdot q + r,$$

ahol $q \in \mathbb{N}$ a hányados, $0 \leq r < b$ pedig a maradék. Ez a felírás egyértelmű (bizonyítsuk be!). Nevezzük át a változókat:

$$a := r_{-1},$$
$$b := r_0,$$

és a korábban említett módon képezzük az euklideszi sorozatot. A következő egyenleteket kapjuk:

$$\begin{aligned}
a := r_{-1} &= q_1 \cdot r_0 + r_1, \\
b := r_0 &= q_2 \cdot r_1 + r_2, \\
r_1 &= q_3 \cdot r_2 + r_3, \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, \\
r_{n-1} &= q_{n+1} \cdot r_n.
\end{aligned}$$

Nézzük az első egyenletet! A maradékos osztás miatt tudjuk, hogy $r_1 < r_0$. Hasonlóan, a második egyenletből $r_2 < r_1$. A gondolatmenetet folytatva:

$$r_{-1} > r_0 > r_1 > \cdots > r_{n-1} > r_n.$$

A természetes számok halmaza alulról korlátos, másképpen szólva előbb-utóbb el kell érnünk a 0-t. Tehát feltehetjük, hogy $r_{n+1} = 0$ valamilyen $n \in \mathbb{N}$ számra, azaz a sorozat véges sok lépésben befejeződik. Az utolsó egyenletből látjuk, hogy r_n osztja a jobb oldalt, így a balt is osztania kell:

$$r_n \mid r_{n-1}.$$

Az utolsó előtti egyenlet jobb oldaláról immár azt is tudjuk, hogy r_n osztja mindkét tagot, így a bal oldalt is osztania kell:

$$r_n \mid r_{n-2}.$$

Az egyenleteken visszafelé haladva ismételjük az előbbi érvelést, így

$$\begin{aligned}
r_n &\mid r_{n-3}, \\
&\vdots \\
r_n &\mid r_0 = b, \\
r_n &\mid r_{-1} = a,
\end{aligned}$$

tehát r_n valóban közös osztó. □

1.2. Állítás. *Az így kapott r_n szám a legnagyobb közös osztó.*

Bizonyítás. Megmutatjuk, hogy bármely közös osztó osztja r_n-t is, tehát r_n-nek a legnagyobbnak kell lennie. Nézzük ismét az euklideszi sorozatot:

$$\begin{aligned}
a := r_{-1} &= q_1 \cdot r_0 + r_1, \\
b := r_0 &= q_2 \cdot r_1 + r_2, \\
r_1 &= q_3 \cdot r_2 + r_3, \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, \\
r_{n-1} &= q_{n+1} \cdot r_n.
\end{aligned}$$

Bármilyen r' közös osztó osztja az első egyenlet bal oldalát ($a = r_{-1}$) és jobb oldalának első tagját ($b = r_0$). Így a jobb oldal második tagját is osztania kell:

$$r' \mid r_1.$$

A következő egyenletekből hasonlóképpen:

$$\begin{aligned} r' \mid r_0, \quad r' \mid r_1 &\Rightarrow r' \mid r_2, \\ r' \mid r_1, \quad r' \mid r_2 &\Rightarrow r' \mid r_3, \\ &\vdots \\ r' \mid r_{n-2}, \quad r' \mid r_{n-1} &\Rightarrow r' \mid r_n. \end{aligned}$$

Így az állítást beláttuk. □

1.2. A kiterjesztett euklideszi algoritmus

1.1. Lemma (Bézout)**.** *A legnagyobb közös osztó*

$$(a, b) = au + bv$$

alakú valamilyen $u, v \in \mathbb{Z}$ számokra.

Bizonyítás. Teljes indukcióval megmutatjuk, hogy az euklideszi sorozatban mindegyik tag ilyen alakú. A sorozat első három tagjából látjuk, hogy

$$\begin{aligned} r_{-1} &= 1a + 0b, \\ r_0 &= 0a + 1b, \\ r_1 &= a - q_1 b. \end{aligned}$$

Tegyük fel, hogy adott $k-2$-re és $k-1$-re az állítás teljesül, azaz

$$\begin{aligned} r_{k-2} &= u_{k-2}a + v_{k-2}b, \\ r_{k-1} &= u_{k-1}a + v_{k-1}b. \end{aligned}$$

Így k-ra a következőt írhatjuk:

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= u_{k-2}a + v_{k-2}b - q_k(u_{k-1}a + v_{k-1}b) \\ &= (u_{k-2} - q_k u_{k-1})a + (v_{k-2} - q_k v_{k-1})b, \end{aligned}$$

ezzel az állítást beláttuk, hiszen r_k is a kívánt alakú. □

Megjegyzés. A továbbiakban

$$ax + by = 1$$

alakú egyenletekkel fogunk foglalkozni, ahol $a, b \in \mathbb{N}$ ismert számok, $x, y \in \mathbb{Z}$ pedig az ismeretlenek. Láttuk, hogy a legnagyobb közös osztóra

$$au + bv = (a, b).$$

A későbbiekben tehát az a és b számokat úgy fogjuk megválasztani, hogy relatív prímek legyenek, azaz $(a, b) = 1$; ebben az esetben a fenti egyenlet az euklideszi algoritmussal megoldható, csak plusz lépésként nyilván kell tartani a Bézout-együtthatók alakulását is.

1.2. Kód. A kiterjesztett euklideszi algoritmus Pythonban:

```
def euk2(a,b):
    u1,u2 = 1,0
    v1,v2 = 0,1
    while b>0:
        q     = a//b
        u1,u2 = u2,u1-q*u2
        v1,v2 = v2,v1-q*v2
        a,b   = b,a%b
    return a,u1,v1
```

2. Csoportelmélet

Itt röviden összefoglaljuk azt, amit a csoportokról tanultunk.

2.1. Csoportaxiómák

2.1. Definíció. A csoport két részből áll: egy G alaphalmazból, és egy ezen értelmezett kétváltozós műveletből. Jelöljük a műveletet a $\odot$ szimbólummal. Ekkor csoportról beszélhetünk, ha:

1. A művelet nem vezet ki a halmazból, azaz ha $g \in G$ és $h \in G$, akkor $g \odot h \in G$.
2. A művelet asszociatív, azaz minden $f, g, h \in G$ elemre $(f \odot g) \odot h = f \odot (g \odot h)$.
3. Létezik $e \in G$ (egységelem), amelyet bármely csoportbeli elemhez „hozzáművelve" magát a elemet kapjuk vissza. Azaz minden $g \in G$-re $e \odot g = g$ és $g \odot e = g$.
4. Minden $g \in G$ csoportelemhez létezik g^{-1} inverz elem, amellyel „összeművelve" az egységelemet kapjuk vissza: $g \odot g^{-1} = e$ és $g^{-1} \odot g = e$.

2.1. Állítás. *Az egységelem egyértelmű.*

Bizonyítás. Tegyük fel, hogy két egységelem is létezik: e és e'. Ekkor

$$e = e \odot e' = e',$$

ahol a 3. axiómát alkalmaztuk kétszer. □

2.2. Állítás. *Minden elemhez az inverz egyértelmű.*

Bizonyítás. A bizonyítás hasonló. Tegyük fel, hogy egy $g \in G$ elemhez két inverz is létezik: g^{-1} és g'.

$$g' \overset{3}{=} g' \odot e \overset{4}{=} g' \odot (g \odot g^{-1}) \overset{2}{=} (g' \odot g) \odot g^{-1} \overset{4}{=} e \odot g^{-1} \overset{3}{=} g^{-1},$$

azaz $g' = g^{-1}$, a két inverz valójában ugyanaz. Az egyenlőségjel feletti számok az alkalmazott axiómát mutatják. □

2.1. Példa. Természetes számok ($\mathbb{N}$) az összeadás műveletével **nem** alkotnak csoportot, mert a 4. axióma nem teljesül.

1. Az összeadás művelete nem vezet ki, két természetes szám összege is természetes szám.
2. Az összeadás asszociatív.
3. Létezik egységelem, hiszen a 0-t bármely természetes számhoz hozzáaadva visszakapjuk a számot.
4. **Nem létezik** minden elemhez inverz, hiszen pl. 2-höz -2-t kellene adnunk, hogy 0-t (egységelemet) kapjunk, de a -2 nem természetes szám.

2.2. Példa. Egész számok ($\mathbb{Z}$) az összeadás műveletével már csoportot alkotnak. A szorzás műveletével azonban **nem**, mert a 4. axióma nem teljesül.

1. A szorzás művelete nem vezet ki, két egész szám szorzata is egész szám.
2. A szorzás asszociatív.
3. Létezik egységelem, hiszen a 1-t bármely egész számhoz hozzászorozva visszakapjuk a számot.
4. **Nem létezik** minden elemhez inverz, hiszen pl. 2-höz $\frac{1}{2}$-t kellene szoroznunk, hogy 1-et (egységelemet) kapjunk, de az $\frac{1}{2}$ nem egész szám.

2.3. Példa. Racionális ($\mathbb{Q}$) és valós ($\mathbb{R}$) számok a szorzással már csoportot alkotnak.

2.2. Egy nagyon fontos csoport

Jelölje $(\mathbb{Z}/n\mathbb{Z})^*$ a modulo n redukált maradékosztályok multiplikatív csoportját. Mit is jelent ez?

- Modulo n. Az n-el való osztás során képződő maradékokat vizsgáljuk.
- Maradékosztály. Végtelen sok olyan egész szám létezik, amely n-nel osztva ugyanazt a maradékot adja. Ezek együttesét nevezzük maradékosztálynak. Például

  $$2 \equiv 9 \equiv 16 \equiv \dots \pmod 7,$$

  mindegyik fenti szám 2 maradékot ad 7-tel osztva, így ezek egy maradékosztályba tartoznak. Minden maradékosztályt jelöljünk pl. a hozzá tartozó legkisebb elemmel, pl. (2) a fenti esetben.
- Redukált maradékosztály. Azon maradékosztályok, amelyek relatív prímek n-hez, azaz legnagyobb közös osztójuk 1 (felírva: $(a, n) = 1$). Adott n-hez redukált maradékosztályok számát megadó függvényt jelöljük $\phi(n)$-nel (Euler-féle függvény).
- Multiplikatív csoport. Műveletnek a szorzást válaszjuk.

2.3. Állítás. *A fenti struktúra valóban csoport.*

Bizonyítás. Az 1. axiómánál azt kell bizonyítanunk, hogy ha $(a, n) = 1$ és $(b, n) = 1$, akkor $(a \cdot b, n) = 1$, azaz a szorzat is része a csoportnak. Ezt az olvasóra bízzuk. A szorzás asszociativitása ismert, a 2.2. példában pedig láttuk, hogy $e = 1$ jó lesz egységelemnek. A 4. axiómánál vegyük észre, hogy

$$aa^{-1} = e \quad \Leftrightarrow \quad aa^{-1} \equiv 1 \pmod n \quad \Leftrightarrow \quad aa^{-1} + nv = 1,$$

amit a kiterjesztett euklideszi algoritmussal könnyen megoldhatunk, így az inverz is létezik. □

2.4. Példa. Modulo 7 redukált maradékosztályok multiplikatív csoportja. Alaphalmaza a 7-hez relatív prím maradékosztályok:

$$1, 2, 3, 4, 5, 6,$$

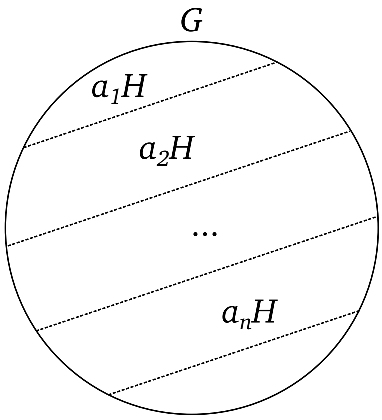
azaz $\phi(7) = 6$. Az egységelem szorzásnál az 1. Melyik elemnek mi az inverze?

- $1 \cdot 1 \equiv 1 \pmod 7$, azaz 1-nek önmaga az inverze,
- $2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$, azaz 2-nek 4 az inverze,
- $3 \cdot 5 \equiv 15 \equiv 1 \pmod 7$, azaz 3-nak 5 az inverze,
- $4, 5$ már szerepelt,
- $6 \cdot 6 \equiv 36 \equiv 1 \pmod 7$, azaz 6-nak önmaga az inverze.

2.5. Példa. Modulo 12 redukált maradékosztályok multiplikatív csoportja. Alaphalmaza a 12-hez relatív prím maradékosztályok, azaz:

$$1, 5, 7, 11,$$

azaz $\phi(12) = 4$. Kiszámolhatjuk, hogy itt minden elemnek önmaga az inverze.



1. ábra. Az a_n elemek H szerinti mellékosztályai „parkettázzák” a csoportot.

2.3. Részcsoportok

2.2. Definíció. H-t G részcsoportjának nevezzük, ha H alaphalmaza részhalmaza G alaphalmazának, és H maga is teljesíti a csoportaxiómákat G műveletére nézve. Jele: $H \leq G$.

2.6. Példa. A páros számok az egész számok additív csoportján belül részcsoportot alkotnak.

2.3. Definíció. Legyen $H \leq G$ részcsoport, valamint $a \in G$. Ekkor $a \odot H$-t úgy képezzük, hogy a-t összeműveljük az összes H-beli elemmel (tehát $a \odot H$ maga is egy halmaz). Ezt nevezzük az a elem H szerinti mellékosztályának.

2.4. Állítás. *Ha $x \in a \odot H$, akkor $a \odot H = x \odot H$, azaz a két mellékosztály megegyezik.*

Bizonyítás. Ha $x \in a \odot H$, akkor biztosan létezik valamilyen $h \in H$ elem úgy, hogy $x = a \odot h$. Számítsuk ki $x \odot H$-t:

$$x \odot H = a \odot h \odot H = a \odot H,$$

hiszen H maga is csoport, így a művelet nem vezethet ki H-ból, azaz $h \odot H = H$. □

2.4. Definíció. A G csoport rendjének nevezzük a csoportban lévő elemek számát. Jele: $|G|$.

2.1. Tétel (Lagrange)**.** *Részcsoport rendje mindig osztója a csoport rendjének.*

Bizonyítás. Legyen G a csoport és $H \leq G$ a részcsoport. Tekintsük az $a \odot H$, $b \odot H$ mellékosztályokat. Ha van közös elemük, pl. $x \in a \odot H$ és $x \in b \odot H$, akkor az előző állítás miatt

$$\begin{aligned} x \in a \odot H &\Rightarrow x \odot H = a \odot H \\ x \in b \odot H &\Rightarrow x \odot H = b \odot H \\ &\Rightarrow a \odot H = b \odot H, \end{aligned}$$

azaz a két mellékosztály megegyezik. A másik lehetőség, hogy a két mellékosztálynak egyáltalán nincs közös eleme. Csak ez a két eset lehetséges, így a H szerinti mellékosztályok „parkettázzák” a csoportot (1. ábra). Számoljuk meg G elemeit:

$$|G| = |a_1 \odot H| + |a_2 \odot H| + \cdots + |a_n \odot H| = \text{valahány} \cdot |H|.$$

Itt felhasználtuk, hogy bármelyik $a_n \odot H$ mellékosztályban pontosan $|H|$ darab elem van. $|H|$-nak osztania kell mindkét oldalt, így a tételt bizonyítottuk. □

Következmény. Prímszámrendű csoportnak nincs valódi részcsoportja, csak önmaga és az egységelemből álló („triviális”) csoport.

2.5. Definíció. Legyen $g \in G$. A

$$H = \{e, \quad g, \quad g \odot g, \quad g \odot g \odot g, \quad \dots\} = \left\{g^0, g^1, g^2, \dots, g^{n-1}\right\}$$

részcsoportot a g elem által generált részcsoportnak nevezzük. Mivel a művelet nem vezethet ki G-ből, véges elemszámú G esetén a fenti séma előbb-utóbb „körbeér”, azaz lesz olyan n, amelyre $g^n = e$. Ha $|H| = |G|$, azaz a részcsoport teljesen kitölti G-t, akkor a G csoportot ciklikusnak nevezzük.

2.6. Definíció. A g által generált csoport rendjét egyúttal a g elem rendjének is nevezzük, ez értelemszerűen megegyezik az előbbi n számmal.

Következmény. Egy elem rendje mindig osztója a csoport rendjének.

2.4. Az Euler–Fermat tétel

Az eddigi eredményeket alkalmazzuk a modulo n redukált maradékosztályok multiplikatív csoportjára. Jelöljük a csoportot G-vel. Tudjuk, hogy az n-hez relatív prím (redukált) maradékosztályok száma $\phi(n)$, így

$$|G| = \phi(n).$$

Válasszunk egy $a \in G$ elemet, amely tehát relatív prím n-hez. Jelöljük a rendjét k-val. Ekkor a 2.1. tételből tudjuk, hogy k osztja $\phi(n)$-t, valamint a rend definíciója szerint

$$a^k \equiv 1 \pmod{n},$$

hiszen szorzásnál 1 az egységelem. Így

$$a^{\phi(n)} \equiv a^{k \cdot q} \equiv (a^k)^q \equiv 1^q \equiv 1 \pmod{n}.$$

Bebizonyítottuk az alábbi tételt:

2.2. Tétel (Euler–Fermat)**.** *Ha a és n egymáshoz relatív prímek, akkor*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

ahol $\phi(n)$ az Euler-féle ϕ-függvény.

Következmény (Kis Fermat-tétel). A fenti feltételekkel egy p prímszámra

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

Bizonyítás. Könnyen látható, hogy prímszámokra $\phi(p) = p - 1$, hiszen p-hez minden nála kisebb pozitív egész szám relatív prím. Innen a tétel azonnal adódik. $\square$

2.7. Példa. Bizonyítsuk be, hogy minden 10-hez relatív prím egész számnak van olyan többszöröse, amely csak 9-esekből áll.

Bizonyítás. Válasszunk tetszőleges n-t, amely relatív prím 10-hez. Ekkor alkalmazhatjuk az Euler–Fermat tételt:

$$10^{\phi(n)} \equiv 1 \pmod{n},$$

így $10^{\phi(n)} - 1$ többszöröse n-nek, és nyilvánvalóan csak 9-esekből áll. $\square$

3. Titkosírás

Most megnézzük a tanultak alkalmazását néhány – jelenlegi tudásunk szerint klasszikus számítógéppel feltörhetetlen – titkosírási sémában.

3.1. RSA titkosírás

Válasszunk két nagy (250-300 jegyű) prímszámot, majd szorozzuk össze őket:

$$pq = n.$$

Tudjuk, hogy egy p prímszámra $\phi(p) = p - 1$, és az is könnyen meggondolható, hogy p, q prímekre

$$\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1).$$

Így $\phi(n)$-t könnyedén ki tudjuk számolni, de ezt titokban tartjuk, és csak n-t tesszük közzé. Ha az u üzenetet szeretné nekünk valaki elküldeni, választ hozzá egy t publikus kulcsot, amely relatív prím $\phi(n)$-hez. Az üzenetet pedig kódolja a következőképpen:

$$r \equiv u^t \pmod{n}.$$

Tehát az információ a következőképpen alakul:

- Mindenki ismeri: r, t, n.
- Csak mi ismerjük: $p, q, \phi(n)$.

Hogyan fejtjük vissza az üzenetet? Kihasználjuk, hogy mi, és csakis mi ismerjük $\phi(n)$-t. Az Euler–Fermat tétel alapján

$$\begin{aligned} u^{\phi(n)} &\equiv 1 \pmod{n}, \text{ } k\text{-adikra emelve} \\ u^{k\phi(n)} &\equiv 1^k \equiv 1 \pmod{n}, \text{ } u\text{-val szorozva} \\ u^{k\phi(n)+1} &\equiv u \pmod{n}. \end{aligned}$$

Tudjuk, hogy a fenti hatványozásból t darabot „már elvégeztek helyettünk”, hiszen nekünk r-t küldték el, és $r \equiv u^t \pmod{n}$. A feladatunk, hogy a „maradék” hatványozást is elvégezzük, és így az előző egyenlet alapján visszakapjuk u-t. Tehát r-t az m-edik hatványra kell emelnünk, ahol

$$tm = k\phi(n) + 1.$$

azaz a

$$tm - k\phi(n) = 1$$

egyenletet kell megoldanunk k-ra és m-re (például a kiterjesztett euklideszi algoritmussal). A p, q prímek kiválasztásához használhatjuk a kis Fermat-tételt:

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

Véletlenszerűen választunk egy 300-jegyű páratlan p számot (ebben a nagyságrendben kb. minden 350. szám prím), majd különböző a értékekkel próbálkozva „teszteljük” a kis Fermat-tételt. Ha mindig 1-t kapunk, a p szám nagyon nagy valószínűséggel prím (kivéve: álprímek, Carmichael-számok).

3.2. Sebezhetőségek

Mikor nem biztonságos az RSA-titkosírás? Az alábbi felsorolás nem teljes:

- Túl közeli p, q számok választása. Ekkor a támadó használhatja a Fermat-faktorizációt.

  3.1. Állítás. *Minden páratlan szám felírható két négyzetszám különbségeként.*

  Bizonyítás.

  $$(k+1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1.$$

  □

  Legyen tehát $n = a^2 - b^2 = (a+b)(a-b)$. A támadónak nincs más dolga, mint különböző a számokkal próbálkozva kiszámítani az $a^2 - n$ számot. Ha ez négyzetszám, akkor megkapta n faktorizációját.

- $p - 1$ és $q - 1$ alacsony prímfaktorokkal rendelkezik. Ekkor a támadó naiv próbálkozással is hamar faktorizálhatja n-t.

- Alacsony t kulcs választása ($u < n^{1/t}$). Ekkor $r = u^t < n$, tehát a maradékos osztás nem játszik szerepet. A támadónak elegendő t-edik gyököt vonnia r-ből. Védekezhetünk ellene az u üzenet véletlenszerű növelésével („padding”), pl. beszúrunk elé egy véletlen hosszúságú $1111\ldots11110$ számot.

- „Chosen plaintext” támadások. A támadó megsejti az üzenet egy részletét (pl. egyes fájlokban a fejléc mindig ugyanolyan szerkezetű), majd véletlenszerű kulcsokkal próbálkozva megpróbálja megfejteni. A padding ez ellen is véd.

- Szoftveres és hardveres támadások. Volt rá példa, hogy az Egyesült Államok hírszerzése szándékosan gyengítette az operációs rendszer ill. hardver véletlenszám-generátorát.

3.3. Egyszerű példa RSA titkosírásra alacsony prímekkel

Legyen a két választott prím $p = 7$ és $q = 11$. Ekkor

$$\begin{aligned} n &= p \cdot q = 77, \\ \phi(n) &= (p-1)(q-1) = 6 \cdot 10 = 60. \end{aligned}$$

A fentiek közül n-t nyilvánosságra hozzuk, a többit titokban tartjuk. Legyen az üzenetünk $u = 3$, azaz például a c betűt szeretnénk titkosítva elküldeni. Ehhez generálunk egy publikus kulcsot, amely relatív prím $\phi(n)$-hez; legyen ez $t = 7$. A t publikus kulcsot szintén nyilvánosságra hozzuk. Most pedig titkosítjuk az u üzenetet a t kulccsal, hogy megkapjuk az r rejtjelezett üzenetet:

$$r \equiv u^t \equiv ? \pmod{n}.$$

Felhasználjuk a gyorshatványozást:

$$\begin{aligned} &3^1 \equiv 3 \pmod{77}, \\ &3^2 \equiv 9 \pmod{77}, \\ &3^4 \equiv 81 \equiv 4 \pmod{77}, \\ &\quad \Rightarrow r \equiv u^t = 3^7 = 3^4 \cdot 3^2 \cdot 3^1 \equiv 4 \cdot 9 \cdot 3 \equiv 108 \equiv 31 \pmod{77}. \end{aligned}$$

Tehát a rejtjelezett üzenetünk $r = 31$. Az megfejtésre vonatkozó egyenletünk a következőképpen néz ki:

$$7m - 60k = 1.$$

Papíron a következőképpen számolhatunk:

$$\begin{aligned}
&& m &= \frac{1+60k}{7} = 9k + \frac{1-3k}{7},\\
x := \frac{1-3k}{7} &\text{ egész kell, hogy legyen} \Rightarrow & k &= \frac{1-7x}{3} = -2x - \frac{x-1}{3},\\
y := \frac{x-1}{3} &\text{ egész kell, hogy legyen} \Rightarrow & x &= 3y+1 \text{ egész.}
\end{aligned}$$

Visszahelyettesítgetve:

$$\begin{aligned}
k &= -2\cdot(3y+1) - \frac{3y+1-1}{3} = -6y-2-y = -7y-2,\\
m &= 9\cdot(-7y-2) + \frac{1+21y+6}{7} = -63y-18+3y+1 = -60y-17,
\end{aligned}$$

Válasszunk olyan y-t, amelyre m pozitív. Pl. $y=-1$, ekkor

$$\begin{aligned}
m &= 43,\\
k &= 5,
\end{aligned}$$

és valóban, $7\cdot 43 - 60\cdot 5 = 1$. A megfejtéshez már csak a

$$31^{43} \equiv u \pmod{77}$$

egyenletet kell megoldanunk. Gyorshatványozással:

$$\begin{aligned}
31^{1} &\equiv 31 \pmod{77},\\
31^{2} &\equiv 37 \pmod{77},\\
31^{4} &\equiv 60 \pmod{77},\\
31^{8} &\equiv 58 \pmod{77},\\
31^{16} &\equiv 53 \pmod{77},\\
31^{32} &\equiv 37 \pmod{77},
\end{aligned}$$

ahonnan

$$31^{43} \equiv 31^{32}\cdot 31^{8}\cdot 31^{2}\cdot 31^{1} \equiv 3 \pmod{77},$$

tehát megfejtettük az üzenetet.

3.4. ElGamal titkosírás

Válasszunk egy G ciklikus csoportot, amelynek a rendje q, és $g\in G$ a generátor elem. Elvégezzük az alábbiakat:

- Választunk egy véletlen x számot 1 és $q-1$ között. Ez lesz a privát kulcsunk, amelyet titokban tartunk.
- Kiszámítjuk a $h=g^x$ elemet. Ezt nyilvánosságra hozzuk; ha valaki titkos üzenetet akar küldeni nekünk, ezt a publikus kulcsot kell használnia. Szintén nyilvánosságra hozzuk q-t, g-t és G-t.

A küldő teendői pedig a következők:

- Ő is választ egy véletlen y számot 1 és $q-1$ között.
- Kiszámítja g^y-t és $h^y = g^{xy}$-t.

- Az üzenetnek megfelelteti a csoport egy m elemét, majd kiszámítja $h^y m$-t. A titkosított üzenet két részből fog állni: $(g^y, h^y m)$.

A megfejtéshez az alábbiakat kell megtennünk:

- A kapott üzenet első felét x-re emeljük, tehát mi is megkapjuk g^{xy}-t.
- Meghatározzuk ennek inverzét: g^{-xy}.
- Most már megfejthetjük az üzenetet a második részből: $g^{-xy}h^y m = g^{-xy}g^{xy}m = m$.

3.5. Egyszerű példa ElGamal titkosírásra

Ciklikus csoportnak vegyük a modulo 29 redukált maradékosztályok multiplikatív csoportját. Mivel 29 prímszám, ezért $q = \phi(29) = 28$. Most szükségünk van egy g elemre, amely az egész csoportot kigenerálja (más szóval, rendje megegyezik a csoport rendjével). Mivel az elem rendje osztója a csoport rendjének, elég 28 osztóira megvizsgálni g rendjét. Próbáljuk meg $g = 2$-t:

$$\begin{aligned} g^4 = 2^4 &\equiv 16 \pmod{29}, \\ 2^7 \equiv 128 &\equiv 12 \pmod{29}, \\ 2^{14} \equiv 16384 &\equiv 28 \pmod{29}, \\ 2^{28} \equiv 28^2 \equiv 784 &\equiv 1 \pmod{29}. \end{aligned}$$

Tehát $g = 2$ rendje valóban 28 (és nem kisebb), azaz g kigenerálja a teljes csoportot. Most választunk egy x-et, legyen mondjuk $x = 4$. Kiszámítjuk:

$$h = g^x = 2^4 \equiv 16 \pmod{29}.$$

Tehát a publikus adatok: $g = 2$, $h = 16$, valamint a G csoport és ennek rendje, q. A feladó megpróbálja elküldeni nekünk a c üzenetet, azaz az $m = 3$ számot. Ehhez választ egy y-t, legyen mondjuk $y = 5$. Kiszámítja:

$$\begin{aligned} h^y = 16^5 &\equiv 23 \pmod{29}, \\ h^y m \equiv 23 \cdot 3 &\equiv 11 \pmod{29} \\ g^y = 2^5 &\equiv 3 \pmod{29}. \end{aligned}$$

Elküldi nekünk a $(g^y, h^y m) = (3, 11)$ üzenetet. A dekódoláshoz mi is kiszámítjuk:

$$\begin{aligned} g^{xy} = (g^y)^x = 3^4 &\equiv 23 \pmod{29}, \text{ azaz} \\ 23t &\equiv 1 \pmod{29} \\ 23t + 29k &= 1, \end{aligned}$$

ahol $t = g^{-xy}$ a keresett inverz. Megoldjuk az egyenletet:

$$\begin{aligned} & & t &= \frac{1-29k}{23} = -k + \frac{1-6k}{23}, \\ z &:= \frac{1-6k}{23} \text{ egész kell, hogy legyen} \Rightarrow & k &= \frac{1-23z}{6} = -4z - \frac{1+z}{6}, \\ v &:= \frac{1+z}{6} \text{ egész kell, hogy legyen} \Rightarrow & z &= 6v - 1 \text{ egész.} \end{aligned}$$

Visszahelyettesítgetve:

$$\begin{aligned} k &= -4 \cdot (6v-1) - \frac{1+6v-1}{6} = -24v + 4 + v = -23v + 4, \\ t &= -(-23v+4) + \frac{1-6(-23v+4)}{23} = 23v - 4 + 6v - 1 = 29v - 5. \end{aligned}$$

Tehát $v = 1$ választással $t = 24$. Tehát $g^{-xy} \equiv 24 \pmod{29}$, így már megfejthetjük az üzenetet:

$$g^{-xy}h^y m \equiv 24 \cdot 11 \equiv 264 \equiv 3 \pmod{29}.$$