

# A számítástudomány alapjai 2017. I. félév

13. gyakorlat. Összeállította: Fleiner Tamás (fleiner@cs.bme.hu)

## Tudnivalók

**Fermat-teszt** Adott  $n$  számról kell eldönteni, prím-e egy véletlen  $1 < a < n$  szám segítségével. Ha  $(n, a) > 1$ , akkor  $n$  nem prím, és  $a$  az  $n$  *leleplezője*, mert egy osztót is megtudunk a segítségével. Ha  $(n, a) = 1$ , akkor ha  $a^{n-1} \not\equiv 1(n)$ , akkor  $a$  az  $n$  *árulója*, és  $n$  bizonyosan nem prím az Euler-Fermat tétel miatt. Míg ha  $a^{n-1} \equiv 1(n)$ , akkor  $a$  az  $n$  *cinkosa*, és  $n$  „valószínűleg” prím.

**Állítás:** Ha  $n$ -nek van árulója, akkor tetsz. mod  $n$  RMR tagjainak legalább a fele áruló.

**Def:** Az  $n$  *Carmichael szám*, ha  $n$  összetett, de nincs árulója.

**Def:** Az  $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  bijekció *egyirányú függvény*, ha  $f$  gyorsan számítható, de az  $f^{-1}$  kiszámítása pusztán  $f$  ismeretében reménytelen. Az  $f$  egyirányú függvény *kiskapus egyirányú függvény*, ha létezik  $f^{-1}$  kiszámítására is hatékony módszer (amit persze pusztán az  $f$ -et számító algoritmus ismeretében reménytelen megtalálni).

**Nyilvános kulcsú titkosítás** Egy  $M$  üzenetet akarunk kódolni. Feltehető, hogy  $M$  egy 0 és  $n$  közötti szám, ami az üzenet ASCII kódjának megfelelő méretű blokkokra darabolásával, és a darabok 2-es számrendszerbeli értelmezésével elérhető. Értelmes konvenció, hogy minden üzenetdarab utolsó néhány bitje random sorozat. A címzett közzéteszi az  $f$  kiskapus egyirányú függvényét, amit bárki könnyen kiszámíthat. Az  $f^{-1}$  hatékony kiszámítására csak a címzett képes. A feladó az  $M$  üzenet helyett az  $X = f(M)$ -t küldjük el, mert ebből egyedül a címzett képes kiszámítani  $f^{-1}(X) = f^{-1}(f(M)) = M$  üzenetet.

**Digitális aláírás** Az  $A$  játékos szeretne  $B$ -nek egy  $M$  üzenetet úgy elküldeni, hogy  $B$  biztos legyen abban, hogy azt  $A$  küldte. Legyenek  $f_A$  ill.  $f_B$  a nyilvános titkosítófüggvényeik. Az  $M$  üzenet  $A$  által aláírt változata  $M' = f_A^{-1}(M)$ . Erről bárki ellenőrizheti az  $f^{-1}(M')$  kiszámításával, hogy az  $M$ -nek az  $A$  által kódolt változatáról van szó, tehát ezt csakis  $A$  írhatta alá. Ha ezt  $B$ -nek titkosítva akarja elküldeni, akkor az  $X = f_B(f_A^{-1}(M))$  üzenetet küldi, amit csak a  $B$  címzett képes megfejteni, hisz  $M = f_A(f_B^{-1}(X))$ .  $B$  mások számára is bizonyítani tudja, hogy az  $M$  üzenetet  $A$  aláírta, mégpedig  $f_B^{-1}(M') = f_A^{-1}(M)$  megadásával, ami az  $A$  által aláírt üzenet.

**Az RSA eljárás** Legyenek  $p, q$  prímelek,  $n = pq$ ,  $m = \varphi(n) = (p-1)(q-1)$ . Legyen  $e > 1$  olyan, amire  $(e, m) = 1$ , és legyen  $d$   $ex \equiv 1(m)$  kongruencia megoldása. A nyilvános kulcs  $(n, e)$ , a titkos kulcs  $(n, d)$ . Az  $f$  kódolófüggvényt az  $M \mapsto M^e \pmod{n}$ , az  $f^{-1}$  dekódolófüggvényt pedig az  $X \mapsto X^d \pmod{n}$  hozzárendelés írja le.

## Gyakorlatok

1. Döntsük el, hogy az 5 cinkosa vagy árulója az  $n = 42$ -nek.
2. Van-e az  $n = 42$ -nek az  $a = 1$ -en kívül cinkosa? (\*) Hát az  $n = 49$ -nek?
3. Igazoljuk, hogy 561-nek nincs árulója, azaz Carmichael szám:  $(a, 561) = 1 \Rightarrow a^{560} \equiv 1(561)$ .
4. Az angol ABC betűit a  $0, 1, \dots, 25$  számok kódolják:  $A = 0, B = 1, \dots, Z = 25$ . Sikerült elfogni az RSA titkosítással kódolt 59, 2, 59, 20, 44, 52 üzenetet, amit a feladó betűnként kódolt az oktondi címzett (85, 43) nyilvános kulcsával. Törjük fel a kódot, fejtsük meg az üzenetet.
5. Bizonyítsuk be, hogy ha az RSA eljárás nyilvános kulcsa  $(n, e)$  a titkos pedig  $(n, d)$ , akkor tetszőleges  $M$  üzenet esetén akkor is jól működik az eljárás, ha  $M$  nem relatív prím  $n$ -hez. Azaz: ha  $X \equiv M^e(n)$ , akkor  $M \equiv X^d(n)$  teljesül tetszőleges  $M$  üzenetre.
6. Legyen  $n = p \cdot q \cdot r$ , ahol  $p, q, r$  különböző prímelek, és legyen  $m = (p-1)(q-1)(r-1)$ , valamint  $(e, m) = 1$ . Jó kódolást kapunk-e az  $(n, e)$  nyilvános kulccsal? Ha igen, akkor határozzuk meg a megfelelő titkos kulcsot.
7. Egy lakattal lezárható ládában szeretnénk titkokat küldeni az ismerősünknek. Sajnos azonban a postás minden olyan küldeményt felnyit, amit csak tud, és amit abban talál, azt ellopja vagy lemásolja. Mindkettőnknek van lakatunk, megfelelő kulcsokkal, de egyikünk sem rendelkezik olyan kulccsal, amihez való lakat a másiknál van. Hogyan oldható meg a biztonságos csomagküldés?
8.  $A$  és  $B$  üzletelnek.  $A$   $k$ -féle információt árul  $B$ -nek, mindegyiket ugyanannyiért.  $B$  úgy szeretne vásárolni, hogy  $A$  ne tudja meg, mire kíváncsi. Hogyan járhatnak el? (\*)