Prímtesztelés, titkosírás

A számítástudomány alapjai
12. gyakorlat

2014. december 12.

1. Döntsük el, hogy van-e közös komplex gyöke a $x^4 + x^3 - 3x - 9$ és az $x^3 - x^2 + x - 6$ polinomoknak.

2. Mutassuk meg, hogy az 561 Carmichael-szám.

3. Milyen veszélyt jelent, ha két RSA eljárással kommunikáló fél közötti lehetséges üzenetek halmaza kicsi, és a támadó számára ismert? Hogyan lehetne védekezni?

4. Az angol ABC betűit a $0, 1, \ldots, 25$ számok kódolják: $A = 0, B = 1, \ldots, Z = 25$. Sikerült elfogni az RSA titkosítással kódolt $59, 2, 59, 20, 44, 52$ üzenetet, amit az oktondi feladó betűnként kódolt a 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 prímek, 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?