SzA XIV. gyakorlat, 2014. december 12.

Titkosan vége a félévnek

Drótos Márton
drotos@cs.bme.hu

Hasznos tudnivalók

- Prímtesztelés: n prím? Random a-ra: $d = (a, n)$; $d \neq 1$: nem; egyébként $a^{n-1} \equiv 1 \pmod{n}$? ha nem: nem prím, egyébként lehet, hogy az – nézzük meg másik a-kra is.
- RSA: p, q prímek (választjuk), $n = pq$, $m = \varphi(n) = (p-1)(q-1)$, $1 \leq e \leq n$ úgy, hogy $(e, m) = 1$ (választjuk), d-hez megoldjuk $ed \equiv 1 \mod m$-et. Nyilvános kulcs: (n, e), titkos kulcs: (n, d). Kódolófüggvény: $f(X) = X^e \mod n$, dekódolófüggvény: $f^{-1}(Y) = Y^d \mod n$.

Feladatok

1. Az órán tanult prímtesztelés segítségével bizonyítsuk be, hogy 8 összetett szám, és 7 valószínűleg prím! Aki szeret sokat számolni, az 561-ről (ami összetett szám, és egyébként a legkisebb Carmichael szám) azt is beláthatja, hogy a módszer szerint valószínűleg prím!
2. Mutassuk meg, hogy az 561 Carmichael szám.
3. Egy pályázat eredményhirdetése előtt néhány nappal a döntőbizottságban ülő egyik tag emailt küldött egyik, megfigyelt ismerősének, melynek tárgya: `Re: Mi lesz az eredmény?`. Úgy tűnik, hogy emberünk és ismerősi köre a szokásosnál tájékozottabb, így hallottak már a titkosításról. Szerencsére az elméleti hátterét a dolognak nem ismerik eléggé, ezért az ismerős nyilvános kulcsa $(85, 43)$, ráadásul úgy tűnik, hogy a szöveg karakterenként van titkosítva. Igazságügyi szakértőként a mi feladatunk, hogy megtudjuk, lehet-e vádat emelni az említett emberek ellen. Az üzenetben a következő számokat látjuk: 58, 48, 27, 3, 6, 48, 67, 76, 38. A (titkosítatlan) karakterkódolás az alábbi táblázat szerint történik:

A	2	B	3	C	4	D	6	E	7	F	8	G	11	H	12	I	13
J	21	K	22	L	23	M	26	N	27	O	28	P	31	Q	32	R	33
S	36	T	37	U	38	V	41	W	42	X	43	Y	46	Z	47		48

4. 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?
5. Tegyük fel, hogy valakivel szeretnék megegyezni egy közös titokban úgy, hogy minden kommunikációnk nyilvános. (Az mindegy, hogy mi lesz a konkrét titok, csak az a lényeg, hogy rajtunk kívül más ne ismerhesse.) Hogyan lehetne ezt megtenni? (Javaslat a gondolkozáshoz: tfh színes festékeket keverünk egymással; ha két festéket összekevertünk, akkor abból az egyes alkotórészeinek színét már nem lehet visszanyerni.)
6. Mese a titkosításokról, igény szerint. (Szimmetrikus, aszimmetrikus, gyakorlati érdekességek, protokollok, veszélyek.)

---

7. 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 $X \equiv M^e \pmod{n}$, akkor $M \equiv X^d \pmod{n}$ teljesül tetszőleges M üzenetre.
8. 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.

9. Fehér kém k féle információt árusít, mindegyiket ugyanolyan áron. Fekete kém szeretné megvenni az egyiket, de úgy, hogy ne derüljön ki Fehér kém számára, hogy melyik volt az (hiszen ellenkező esetben Fehér kém elkezdene egy $k+1$-edik információt is árulni: vajon mi érdekli Fekete kémet?). Adjunk protokollt, ami alapján kölcsönös megelégedéssel végezhetik el a tranzakciót!

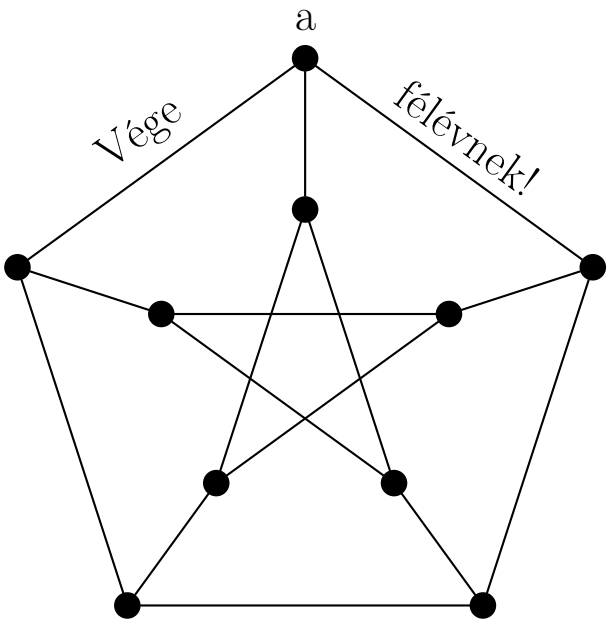
---

10. Igény szerint kérdések feltevése a gyakvezérnek, pl. email segítségével.

11. Tanulás. Megértés.

12. ???

13. Profit! (Jól sikerült vizsga. Öröm.)



Köszönöm a figyelmet!