NÉV: NEPTUN:

ELTE IK Diszkrét modellek alkalmazásai (BSc, 18, F) A feladatsor

1. zárthelyi dolgozat

I. rész (hagyományos, papíron megoldandó feladatok)
Felhasználható idő: 20 perc

1. feladat 15 pont
Shamir titokmegosztással az $S = 11$ titkot osszuk szét 6 ember között, ahol legalább 2 ember legyen szükséges az eredeti titok előállításához. A titokmegosztáshoz használt polinom főegyütthatója 5 legyen. Ezen paraméterek ismeretében válassza modulusnak a lehető legkisebb alkalmas prímszámot. Az 1 és 4 kezdetű titokrészletekből állítsuk elő az eredeti titkot Lagrange-interpolációval.

II. rész (programozási feladatok)
Felhasználható idő: 70 perc

2. feladat 10 pont
Írjon *foo(original, pattern, change)* szignatúrával függvényt, amely visszatér az *original* sztring egy olyan másolatával, amelyben lecseréli a *pattern* **utolsó előtti** előfordulását *change*-re. Ha *pattern* nem található meg legalább kétszer *original*-ban, akkor a függvény térjen vissza üres sztringgel. Például, a *foo("This string/string is my dummy string in this exercise about strings.", "string", "FOO")* függvényhívásra a helyes eredmény: *This string/string is my dummy FOO in this exercise about strings.*

3. feladat 7 pont
Az Agoh–Giuga-sejtés szerint egy $p > 1$ természetes szám prímszám akkor és csak akkor, ha $1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1} + 1$ osztható p-vel. Írjon SageMath programot, amely megmutatja, hogy a $[2; 1000]$ intervallumban **nem létezik** olyan szám, amelyre a sejtés téved.

4. feladat 6 pont
Az

```
RcazVYTG23g8XVHnqh_NZXRt8W3mVDympNuMqTLVQCpA__@MPxXTZxrYaArT.Pw97VQ6n5N4whkRgzf
Uc@st___JThAa2R874
```

jelszóhoz készítsen titokrészleteket, amelyet 30 ember között osztunk szét úgy, hogy legalább 12 ember szükséges legyen az eredeti jelszó előállításához. A jelszót reprezentálja 128-as alapszámú számrendszerbeli számként. Mutassa be, hogy 12 titokrészletből az eredeti jelszó előállítható, azonban 11-ből nem.

5. feladat 12 pont
Módosítsa az *SSS_secret_pieces_from_primenum_and_coeffs(num_of_people, secret, primenum, coeff)* függvényt úgy, hogy paraméterként vegyen át egy *epsilon* egész számot is. Ha *epsilon* negatív, akkor a függvény dobjon *ValueError* kivételt. A függvény úgy állítson elő titokrészleteket, hogy ha az éppen előállított titokrészlet bármelyik komponense a titok *epsilon* sugarú környezetében van, akkor ezt a titokrészletet ne használja. Vigyázzon arra, hogy a függvény továbbra is *num_of_people* darab titokrészletet állítson elő. Ha a kapott paraméterekkel nem lehetséges *num_of_people* darab titokrészletet előállítani, a függvény dobjon *ValueError* kivételt. Hívja meg a függvényt két példával: egyszer amikor sikeresen előállít *num_of_people* darab titokrészletet, és egyszer amikor nem lehetséges ennyi titokrészletet előállítani. Emlékeztetőül: Az x szám az A szám *epsilon* sugarú környezetében van, ha $|x - A| \leq epsilon$.

2021. november 10.
Koch-Gömöri Richárd, kgomoririchard@inf.elte.hu, kgomori.richard@gmail.com