1. zárthelyi dolgozat

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

1. feladat 10 pont
Határozza meg Euklideszi-algoritmussal az (a) $lnko(130, 74)$ (b) $lnko(29, 32)$ értékeket. Oldja meg a következő lineáris kongruencia egyenleteket:
(c) $15x \equiv 3 \pmod{10}$ (d) $12x \equiv 6 \pmod{21}$

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

2. feladat 5 pont
Írjon *split_string_to_maxlen_pieces(string, piece_maxlen)* szignatúrával függvényt, amely a paraméterként kapott *string* szöveget *piece_maxlen* hosszúságú darabokra vágja, majd visszatér ezen darabok listájával.

3. feladat 10 pont
Implementálja a következő szimmetrikus kulcsú titkosítást: Az ABC az angol kis- és nagybetűket tartalmazza; az $encrypt(plaintext, key)$ függvény *plaintext* paramétere a titkosítandó sztring, *key* pedig egy pozitív természetes szám, amely 1-gyel hosszabb, mint *plaintext*. A titkosító függvény a *plaintext* betűit a *key* megegyező pozícióján lévő számjeggyel tolja el az ABC-ben, majd a *key* utolsó számjegyével forgatja körbe az előállított sztringet, így visszatérve a kapott cipher-rel.

Például, ha a plaintext "alma", a *key* pedig 12341, akkor az "a" betűt 1-gyel, az "l" betűt 2-vel tolja el stb., így kapva a "bnpe" sztringet. Ezt a "bnpe" sztringet pedig 1-gyel forgatja körbe, a kapott végeredmény cipher így pedig "ebnp". Az ABC utolsó betűje után az ABC első betűje következzen.

Implementáljon $decrypt(ciphertext, key)$ szignatúrával visszafejtő függvényt is.

Ha a függvények *key* paramétere negatív szám, vagy ha nem megfelelő hosszú, akkor a függvények dobjanak $ValueError$ kivételt. Mutassa be a titkosítás működését egy példán.

4. feladat 10 pont
Írjon $gen\_RSA\_public\_key(modulus\_len)$ szignatúrával függvényt, amely paramétere *modulus_len* pozitív egész szám (különben dobjon $ValueError$ kivételt). A függvény válasszon két alkalmas, egymást követő p_1, p_2 prímszámokat (lehet véletlenszerűen, de nem elvárás), majd a választott prímszámokból generáljon RSA publikus kulcsot, ahol a modulus számjegyeinek száma (tízes számrendszerben) legalább *modulus_len*. A $gen\_RSA\_public\_key(10)$ egy lehetséges helyes eredménye: $(1000773161, 5)$.

5. feladat 5 pont
A 96171878201631844186130500275174019949164822666548549304878427832449001 35 cipher előállításához a
(10577795823851879016615591732095183350836585707548354280149683226062077461, 425771351)
RSA publikus kulcsot használták. A publikus kulcs előállításához használt egyik prímszám 3252352352352352215325321499552352523 volt. (Az adatok megtalálhatóak a ZH Cocalc munkafüzetében.) A modulus faktorizálásával törje fel a titkosítást: mi volt az eredeti szöveges üzenet?

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