2. zárthelyi dolgozat

I. rész (hagyományos, papíron megoldandó feladatok)
Felhasználható idő: 30 perc

1. feladat 12 pont
Shamir titokmegosztással az $S = 7$ titkot osszuk szét 5 ember között, ahol legalább 2 ember legyen szükséges az eredeti titok előállításához. A titokmegosztáshoz használt polinom főegyütthatója 4 legyen. Ezen paraméterek ismeretében válassza modulusnak a lehető legkisebb alkalmas prímszámot. Az 2 és 5 kezdetű titokrészletekből állítsuk elő az eredeti titkot Lagrange-interpolációval.

2. feladat 3 pont
A $p_1 = 7$, $p_2 = 11$ prímszámokat használva generáljon RSA publikus kulcsot, amelynek egyik komponense sem p_1 vagy p_2.

II. rész (programozási feladatok)
Felhasználható idő: 90 perc

3. feladat 10 pont
(a) Írjon *Caesar_encrypt(plain, shift)* szignatúrával függvényt, amely Caesar-titkosítással (Caesar-rejtjelezéssel) titkosítja a *plain* szöveget *shift* eltolással.
(b) Írjon *Caesar_decrypt(cipher, shift)* szignatúrával függvényt, amely Caesar-titkosítással (Caesar-rejtjelezéssel) visszafejti a *cipher* szöveget, amelyet *shift* eltolással titkosítottak.
(c) Mutassa be a függvények működését az "árvíztűrő tükörfúrógép" sztringen, ahol az eltolás legyen 4.

4. feladat 10 pont
Írjon *split_string_to_maxlen_pieces(string, piece_max_len)* szignatúrával függvényt, amely a paraméterként kapott *string* szöveget *piece_max_len* hosszúságú darabokra vágja, majd visszatér ezen darabok listájával.

5. feladat 15 pont
A gyakorlaton megírt *SSS_secret_parts()* függvény nagyon hosszú sztringekre igen nagy számokkal dolgozik, ami lassúvá teszi a függvény működését, ezért hosszú sztringek titokmegosztásakor kisebb darabokra vágják az eredeti sztringet, majd a darabokat külön-külön titokmegosztják. Ebben a feladatban írunk egy olyan függvényt, amely hosszú sztringeket darabokra vág, mindegyik darabhoz titokrészleteket állít elő, majd összeállítja az egyes résztvevőknek odaadandó információkat.

Írjon *SSS_share_string(required_num_of_people, num_of_people, string, piece_max_len)* szignatúrával függvényt, amely a *string* sztringet *piece_max_len* hosszúságú darabokra vágja (ehhez felhasználhatja a *split_string_to_maxlen_pieces()* függvényt; ha nem sikerült megvalósítania ezt a függvényt, akkor a *split_string_to_maxlen_pieces()* függvénye ebben a feladatban térjen vissza beégetett sztringek listájával), majd minden sztring darabhoz (256-os számrendszerbeli számként értelmezve) titokrészleteket állít elő a gyakorlaton megírt *SSS_secret_parts()* függvénnyel.

Ekkor minden sztring darabhoz külön-külön előáll egy prímszám és egy lista, amely *num_of_people* darab titokrészletet tartalmaz. A függvény térjen vissza egy olyan listával, amelynek tartalma *num_of_people* darab rendezett pár: [(1. ember), (2. ember), ...]

Egy ilyen rendezett pár első komponense a résztvevő sorszámát (a gyakorlatokról ez az i), a rendezett pár második komponense pedig egy lista, amely az adott i-hez tartozó polinomok helyettesítési értékeit tartalmazza: [(1, [...]), (2, [...], ...))]. Mivel mindegyik polinomhoz külön prímszám tartozik, ezért ez a lista tartalmazzon rendezett párokat, amelynek első komponense a prímszám, második komponense a polinom i helyen felvett helyettesítési értéke.

Például, az *SSS_share_string(4, 6, "abc", 2)* függvényhívás egy lehetséges eredménye:
2 sztring darab:

"ab" titokmegosztása: (2155451, [(1, 456951), (2, 1408707), (3, 724753), (4, 560546), (5, 916092), (6, 1791397)])
"c" titokmegosztása: (809, [(1, 417), (2, 480), (3, 294), (4, 674), (5, 8), (6, 729)])

ekkor a végeredmény: [(1, [(2155451, 456951), (809, 417)]), (2, [(2155451, 1408707), (809, 480)]), (3, [(2155451, 724753), (809, 294)]), (4, [(2155451, 560546), (809, 674)]), (5, [(2155451, 916092), (809, 8)]), (6, [(2155451, 1791397), (809, 729)])]

A példa csak minta, az *SSS_secret_parts()* függvénybe épített véletlenszerűség miatt az eredmény minden hívásnál más lesz.

A *SSS_share_string()* függvénnyel készítsen titokrészleteket a *longstr* sztringhez (*longstr* a zh SageMath munkafüzetben megtalálható), amit 6 embernek osztunk osztunk szét, ahol legalább 5 ember legyen szükséges az eredeti sztring előállításához. Az eredeti sztringet darabolja 64 méretű részekre.

longstr = """Fox Mulder: We wanted... to believe. We wanted to call out. On August 20th and September 5th, 1977, two spacecraft were launched from the Kennedy Space Flight Center, Florida. They were called Voyager. Each one carries a message. [...] A gold-plated record depicting images, music and sounds of our planet, arranged so that it may be understood if ever intercepted by a technologically mature extraterrestrial civilization. Thirteen years after its launch, Voyager One passed the orbital plane of Neptune and essentially leaving our solar system. Within that time, there were no further messages sent. Nor are any planned. We wanted to listen. On October 12th, 1992, NASA initiated the high-resolution microwave survey. A decade long-search by radio telescope, scanning ten million frequencies for any transmission by extraterrestrial intelligence. Less than one year later, first-term Nevada Senator R. B. successfully championed an amendment which terminated the project. I wanted to believe but the tools have been taken away. The X-Files have been shut down. They closed our eyes. Our voices have been silenced... our ears now deaf to the realms of extreme possibilities. [The X-Files, season 2, episode 1: 'Little Green Men', 1994]"""

(A *SSS_share_string()* 20 másodperc alatt terminál, a *SSS_secret_parts()* függvény percek alatt sem.)

2020. december 17.
Koch-Gömöri Richárd, kgomoririchard@inf.elte.hu, kgomori.richard@gmail.com