Криптографија

Задаци за рад по групама

Група III

Задатак ове групе је да направи програм за RSA енкрипцију и декрипцију.

Задатак 1.

Циљ овог програма је енкрипција и декрипција RSA алгоритмом.

Кориснику се мора обезбиједити начимн да генерисање простих бројева p и q. Потом омогућити кориснику и да помножи дате борјеве и добије неки број N. Такође, за избор експонента e потребно је провјерити да ли је овај број узајамно прост са $\phi(N)$.

---

rsa_enc

Улаз: број за енкрипцију: x, N, e
(**N** је број добијен као производ два проста броја p і q,
а **e** је експонент за енкрипцију)
Излаз: број x'
(Енкрипција RSA алгоритмом)

У следећем програму, корисник врши декрипцију доспјелог криптограма. Корисник (симулација Алисе која врши декрипцију) мора да обезбиједи тајни експонент d, као и N као улазне податке.

---

rsa_dec

Улаз: број x', N, d
(**d** је тајни кључ - експонент за декрипцију)
Излаз: број x
(Декрипција RSA алгоритмом)

Напомена: Сви програми се обједињују у оквиру јединственог корисничког интерфејса. Сваки програм мора бити user-friendly са прецизним упуствима просјечном кориснику. За пројекат је потребно направити одговарајућу **документацију**. Документација подразумијева

1. Псеудо-код за сваки од потребних програма.
2. Прецизна упуства потенцијалним корисницима како се користе поједини програми, шта они раде и која су им ограничења.
3. Описати поступак рада групе и назначити сваки појединачни допринос чланова групе.
4. Написати предлог побољшања постојећих програма.
5. Указати на могуће недостатке у прецизности формулације постављених задатака.

Документацију доставити у склопу пројекта у електронској форми.