RSA kriptografija

Jūsų užduotis bus realizuoti RSA kriptografijos algoritmą ir įvykdyti ataką prieš blogai parinktą viešąjį raktą.

Instrukcijos

RSA algoritmas ir galimi nulaužimo būdai yra aprašyti William Stein knygoje „Elementary Number Theory: Primes, Congruences, and Secrets“ 3 skyriuje. Knyga yra laisvai prieinama: http://wstein.org/ent/. Galite naudoti bet kurią programavimo kalbą, bet RSA algoritmą turėtumėte įgyvendinti patys (negalima naudotis kriptografijai skirtomis bibliotekomis). Kadangi Stein knygoje yra pateikti Sage programų kodai, jums gali praversti Sage cloud'as: https://cloud.sagemath.com.

Užduotis

Faile https://www.dropbox.com/s/75s0eaoqm6hcoru/public%20keys?dl=0 yra duotas viešasis raktas (e, n) ir šifruotas tekstas (cyphertext). Pasitikrinimui nurodyta viena žinutės ir šifruoto teksto pora. Žinutė paverčiama į skaičių kaip aprašyta knygoje (3.3.2 Encoding a Phrase in a Number), tada užšifruojama RSA algoritmu. Šifruotą tekstą reiktų iššifruoti pagal RSA ir tada iš skaičiaus paversti į tekstą. Iššifruotą žinutę ir programos kodą reikia atsiųsti man `jonas.siurys@mif.vu.lt` iki semestro pabaigos (per sesiją atsiųstų darbų nevertinsiu).