Taikomosios algebros kursinis darbas.

Tema 2.
Viešojo rakto algoritmai: RSA algoritmas – teorija, realizacija, šifro saugumas

1.**Metodo apžvalga**: viešojo rakto algoritmų bendroji schema, apžvalga.

2. **RSA algoritmas.**

Teorinė dalis: pateikti kiekvieno etapo algoritmus, aptarti jų teisingumo teorinius įrodymus.

Eksperimentinė dalis: realizuoti RSA algoritmą, pateikti kiekvieno etapo tarpinius rezultatus pasirinktam/pateiktam raktui.

Pranešimas yra įvedamas HEX formatu.

3. **Tekstinio pranešimo šifravimas:** tekstas įvedamas įprastiniu formatu. Jį koduojame ASCI formatu ir saugome HEX formatu. Ilgesnių nei 64 bitų pranešimų šifravimui naudojame blokinį CBC algoritmą.

4. **RSA šifravimo algoritmo saugumas.** Atlikite skaičiavimo eksperimentus ir patikrinkite kokio ilgio raktą galite "nulaužti" per 5 minutes.

Kaip "nulaužti" RSA raktą greičiau?

5. **Išvados.**

6. **Literatūros sąrašas.**