Taikomosios algebros kursinis darbas.

Tema 3.
Pasikeitimo šifravimo raktais algoritmai: Diffie-Hellman algoritmas, ElGamal šifravimo schema

1.**Metodo apžvalga**: pasikeitimo raktais algoritmų svarba, apžvalga.

2. **Diffie-Hellman algoritmas.**

Teorinė dalis: pateikti kiekvieno etapo algoritmus, aptarti algoritmo teisingumo teorinius įrodymus. Diskretusis logaritmavimas (DL), uždavinio sudėtingumas. Algoritmai, skirti DL skaičiavimui .

Eksperimentinė dalis: realizuoti kurį nors algoritmą, skirtą DL uždavinio sprendimui, pateikti rezultatus.

3. **ElGamal šifravimo algoritmas.**

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

Pranešimas yra įvedamas HEX formatu.

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

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

Kaip "nulaužti" raktą greičiau?

6. **Išvados.**

7. **Literatūros sąrašas.**