Taikomosios algebros kursinis darbas.

Tema 1.
DES šifravimo algoritmas: teorija, realizacija, šifro saugumas

1.**Metodo apžvalga**: blokiniai šifravimo algoritmai, Feistel šifravimo algoritmų bendroji schema.

2. **DES algoritmas.**

Teorinė dalis: pateikti kiekvieno etapo algoritmus, aptarti jų sudėtingumą.

Eksperimentinė dalis: realizuoti DES algoritmą, pateikti kiekvieno etapo tarpinius rezultatus pasirinktam/pateiktam raktui ir 64 bitų ilgio pranešimui.

Raktas ir pranešimas yra įvedami 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 ECB algoritmą.

4. **DES šifravimo algoritmo saugumas.** Atlikite skaičiavimo eksperimentus ir patikrinkite kokio ilgio rakto bloką galite perrinkti per 5 minutes.

Kaip "nulaužti" DES raktą greičiau?

5. **Išvados.**

6. **Literatūros sąrašas.**