**1. Įgyvendinto algoritmo numeris, pavadinimas**

**Nr. 4 – BLAKE2 (variantas: BLAKE2s)**  
Šis algoritmas parinktas dėl paprastesnės struktūros, lyginant su BLAKE2b, ir tinkamumo 32 bitų sistemoms bei greito veikimo.

**2. Kas įgyvendinta, o kas ne**

* ✅ Įgyvendinta pilna BLAKE2s maišos funkcija pagal oficialią RFC 7693 specifikaciją.
* ✅ Realizuota kompresavimo funkcija su visais 10 raundų ir SIGMA permutacijomis.
* ✅ Programa skaito įvesties failą baitais, apskaičiuoja hash reikšmę ir ją išveda šešioliktainiu formatu.
* ✅ Parametrai perduodami per komandinės eilutės argumentus.
* ✅ Įgyvendintas paskutinio bloko apdorojimas ir žymėjimas kaip final block (f = True).
* ❌ Nerealizuota slapto rakto (keyed hashing) versija ar kiti papildomi parametrai, kadangi to nereikalavo užduotis.

**3. Instrukcija, kaip paleisti programą, kokie jos parametrai**

**Paleidimas terminale:**

python main.py <įvesties\_failas> [išvesties\_failas]

**Pavyzdys:**

python main.py test.txt >> Išves maišos reikšmę į ekraną.

python main.py test.txt rezultatas.txt >> Įrašys maišos reikšmę į rezultatas.txt.

**4. Laiko sąnaudos (neprivaloma, bet pageidautina)**

| **Etapas** | **Laikas (val.)** |
| --- | --- |
| Dokumentacijos skaitymas | 2 |
| Projektavimas | 1 |
| Programavimas | 4 |
| Testavimas ir klaidų taisymas | 2 |
| Ataskaitos ruošimas | 1 |
| **Iš viso** | 10 |

**5. Iššūkiai ir sudėtingiausios vietos**

* Sudėtingiausia buvo teisingai suprasti kompresavimo funkcijos logiką – kaip teisingai atlikti G funkcijos operacijas ir bitų rotacijas.
* Taip pat iššūkį kėlė teisingas t skaitiklio (baitų skaičiaus) skaičiavimas ir finalo (f) žymėjimas paskutiniame bloke.
* Kita sudėtinga dalis buvo teisingai valdyti baitų blokų padalijimą ir jų konvertavimą į 32 bitų žodžius.

**6. Naudoti informacijos šaltiniai**

* RFC 7693: The BLAKE2 Cryptographic Hash and MAC
* <https://blake2.net/>
* Užduotyje pateikti reikalavimai ir dėstytojo paskaitų skaidrės

**7. Priedai (programos failai)**

Pridėti šie failai:

* main.py – programa, paleidžianti maišos funkciją su failais
* blake2.py – BLAKE2s algoritmo realizacija
* (neprivaloma) test.txt – pavyzdinis įvesties failas