**A machine with blue light coming out of it

Description automatically generated**

**Skyrius 1: Senovės pasaulio šifrai**

**Apžvalga:** Nuo pat seniausių laikų žmonės naudojo slaptus kodus ir šifrus, kad saugotų savo žinias ir paslaptis. Senovės Egipte, Grėtijoje ir Romoje kriptografija buvo naudojama kariniais tikslais ir politinėje komunikacijoje.

**Pagrindiniai momentai:**

* **Egipto hieroglifai** – nors tai ne visada buvo naudojama kaip kriptografija, kai kuriuos hieroglifus tik iniciuoti žmonės galėjo skaityti ir suprasti.
* **Skitalė** – viena seniausių žinomų šifravimo priemonių, naudota senovės Graikijoje. Tai buvo medinė ritė, ant kurios rašant žodžiai būdavo užšifruojami.

**Skyrius 2: Viduramžių kriptografija**

**Apžvalga:** Viduramžiais, su raštingumo plitimu ir valstybių formavimusi, kriptografija tapo svarbi diplomatijoje ir karo strategijoje.

**Pagrindiniai momentai:**

* **Alberti diskas** – sukurtas Leon Battista Alberti, laikomas pirmuoju tikru mechaniniu šifravimo įrenginiu.
* **Vigenère šifras** – sudėtingesnis polialfabetinis šifras, kurį ilgą laiką laikė nepažeidžiamu.

**Skyrius 3: XX amžiaus kriptografija ir jos vaidmuo karuose**

**Apžvalga:** Dvi pasaulio karai buvo kriptografijos vystymosi aukso amžius, kai abiejų konfliktų šalys intensyviai naudojo šifrus ir kodo laužytojus.

**Pagrindiniai momentai:**

* **Enigma mašina** – Vokietijos kariuomenės naudota mašina, kuri buvo pagrindinis kriptografijos įrankis Antrojo pasaulinio karo metu.
* **Alan Turing** – matematikas, kuris sukūrė mašiną, galinčią laužyti Enigma kodus, žymiai prisidėjo prie karo eigų pakeitimo.

**Skyrius 4: Moderni kriptografija**

**Apžvalga:** Šiuolaikinė kriptografija apima tiek klasikinę simetrinę kriptografiją, tiek modernią asimetrinę kriptografiją, kuri leidžia saugius sandorius ir komunikaciją internete.

**Pagrindiniai momentai:**

* **RSA algoritmas** – pirmasis viešai prieinamas asimetrinio šifravimo algoritmas.
* **Blockchain ir kriptovaliutos** – naujausios kriptografijos aplikacijos, keičiančios mūsų supratimą apie pinigus ir sandorius internete.

**Skyrius 5: Kriptografijos ateitis ir iššūkiai**

**Apžvalga:** Naujos technologijos, tokios kaip kvantiniai kompiuteriai, žada pakeisti kriptografijos peizažą, kurdamos tiek naujas šifravimo galimybes, tiek grėsmes esamoms technologijoms.

**Pagrindiniai momentai:**

* **Kvantinė kriptografija** – naudoja kvantinius mechanizmus, kad pasiūlytų naują saugumo lygį, kurį praktiškai neįmanoma pažeisti naudojant tradicinius metodus.
* **Privatumo ir saugumo iššūkiai** – kaip balansuoti tarp saugumo ir vartotojų privatumo interneto eroje.