VILNIUS = yra mokykla

Wjmojvt zsb nplzlmb

Iššifruok Vilniaus kodą

Pamokos medžiaga

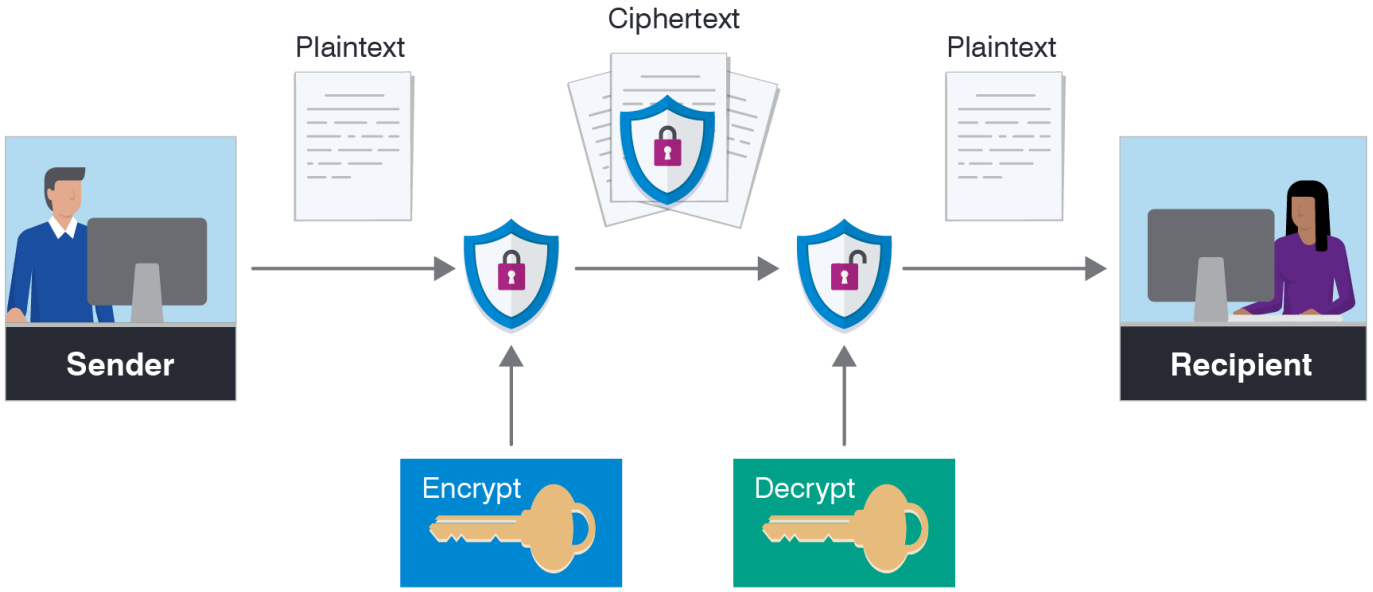
Pamoką sukūrė Ina Kovaliova projektui „Vilnius yra mokykla“

Pamokos tikslai ir uždaviniai

- **Supažindinsime** su šifravimo sistemų istorija ir principais
- **Ugdysime** gebėjimą atpažinti ir naudoti skirtingus šifravimo metodus
- **Suteiksime** žinių apie Vilniaus istoriją ir kultūrą
- **Skatinsime** komandinį darbą, problemų sprendimą ir kūrybiškumą

Kas yra šifravimas?

Informacijos užkodavimo procesas, siekiant apsaugoti ją nuo neįgaliotų asmenų.



Different keys are used to encrypt
and decrypt messages

Šifravimo istorija

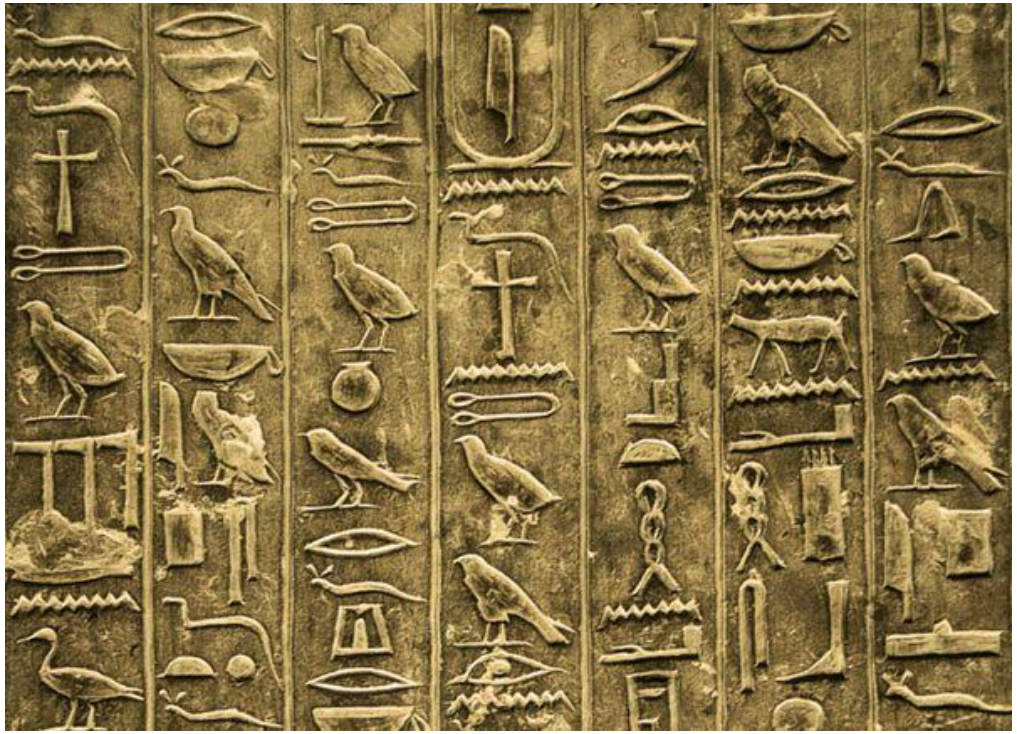
- Senovės civilizacijos ir jų šifrai
- Šifravimo mašinos
- Šiuolaikinis šifravimas ir jo taikymas

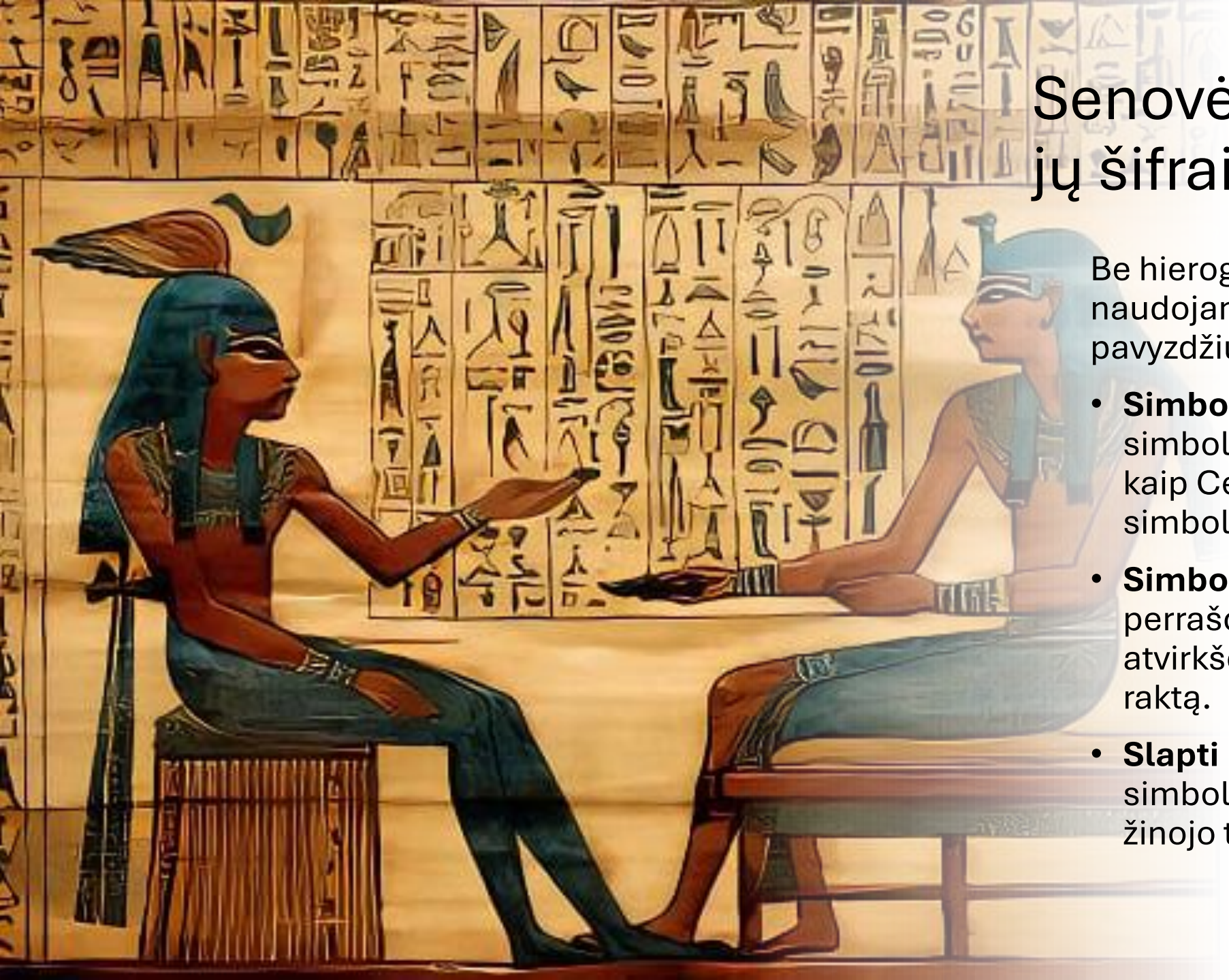
Senovės civilizacijos ir jų šifrai

Senovės Egipte buvo naudojami **hieroglifai**, kurie yra sudėtinga rašto sistema, apimanti *ideogramas*, *fonogramas* ir *determinatyvus*.

Nors hieroglifai nebuvo sukurti specialiai šifravimui, jų sudėtingumas ir simbolinis pobūdis kartais apsunkindavo tekstų supratimą tiems, kurie nebuvo su jais susipažinę.

Tai galima laikyti tam tikra šifravimo forma.





Senovės civilizacijos ir jų šifrai

Be hieroglifų, senovės Egipte buvo naudojami ir kiti šifravimo metodai, pavyzdžiui:

- **Simbolių pakeitimas:** Vienas simbolis pakeičiamas kitu, panašiai kaip Cezario šifre, bet su didesne simbolių įvairove.
- **Simbolių perrašymas:** Simboliai perrašomi kita tvarka, pavyzdžiui, atvirkščiai arba pagal tam tikrą raktą.
- **Slapti kodai:** Naudojami specialūs simboliai arba ženklai, kurių reikšmę žinojo tik tam tikras žmonių ratas.

Šifravimo mašinos

Šifravimo mašinos yra svarbus etapas šifravimo istorijoje, žymintis perėjimą nuo rankinio prie mechaninio ir vėliau elektroninio šifravimo. Jos padėjo užtikrinti saugesnį ir efektyvesnį informacijos perdavimą, ypač karo metu.

Enigma

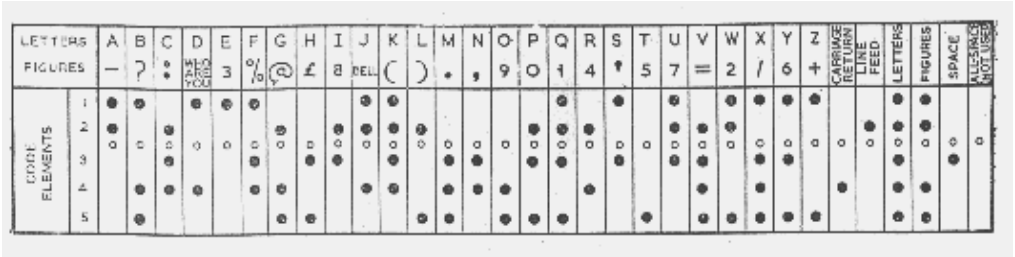
- Enigma buvo sukurta Vokietijoje 1920-aisiais.
- Elektromechaninė rotorinė mašina, kurioje raidės šifruojamos naudojant besisukančius rotorius ir elektros grandines. Kiekvienas rotoriaus pasukimas pakeisdavo šifravimo raktą, todėl Enigma buvo labai sudėtinga nulaužti.
- Plačiai naudota Vokietijos kariuomenės Antrojo pasaulinio karo metu.
- Britų matematikai ir kriptografai, vadovaujami Alano Turingo, sėkmingai nulaužė Enigmos kodą, kas turėjo didelę įtaką karo eigai.
- Yra išlikę veikiančių Enigmos mašinų, kurias galima pamatyti muziejuose arba privačiose kolekcijose. Taip pat yra sukurta kompiuterinių Enigmos simuliatorių, kuriuos galima išbandyti internete.

https://www.101computing.net/enigma-machine-emulator/

Kitos šifravimo mašinos

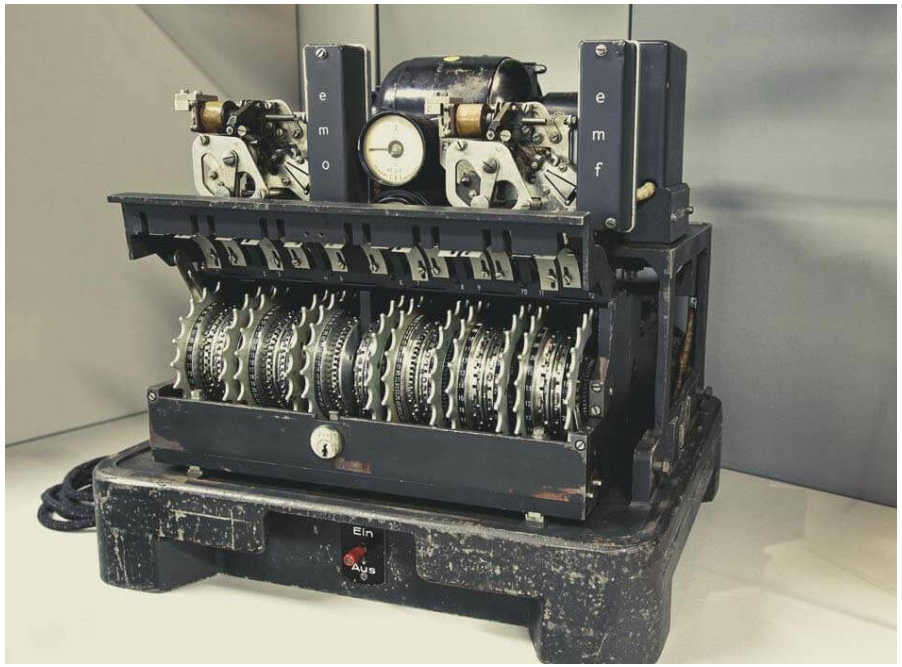
- **Lorenz šifras:** Vokiečių kariuomenės naudota šifravimo mašina, skirta aukšto lygio pranešimams šifruoti. Buvo dar sudėtingesnė už Enigmą.
- **SIGABA:** Amerikiečių kariuomenės naudota rotorinė šifravimo mašina, laikoma viena saugiausių Antrojo pasaulinio karo metu.
- **Typex:** Britų kariuomenės naudota rotorinė šifravimo mašina, panaši į Enigmą.

Lorenz šifras



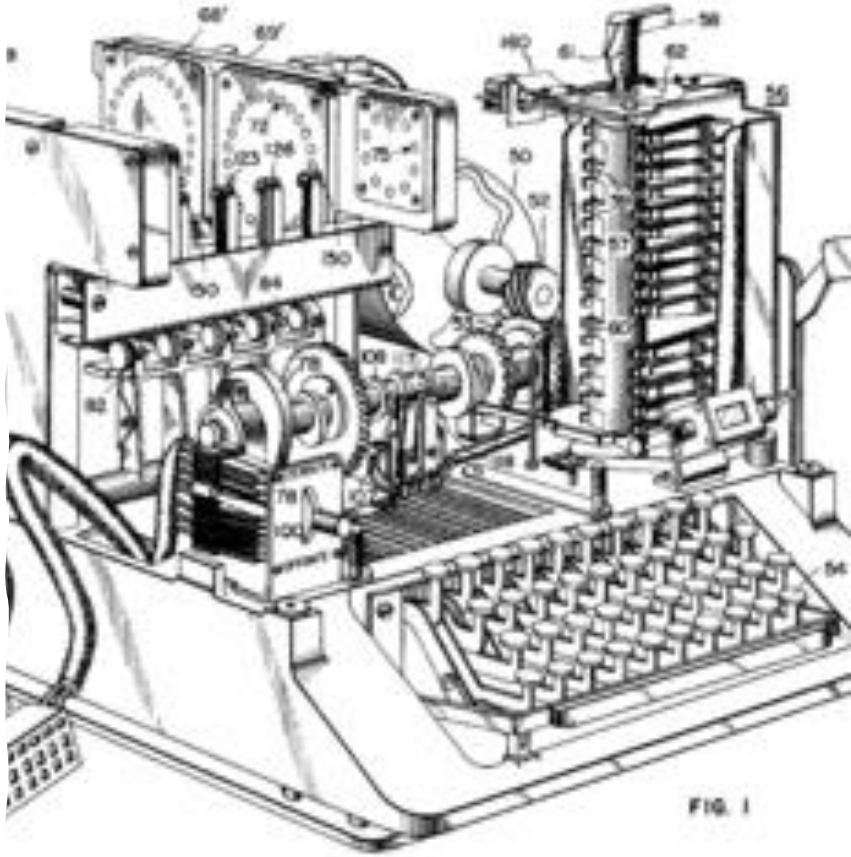
LETTERS / FIGURES	A / –	B / ?	C / :	D / WHO ARE YOU	E / 3	F / %	G / @	H / £	I / 8	J / BELL	K / (	L /)	M / .	N / ,	O / 9	P / 0	Q / 1	R / 4	S / '	T / 5	U / 7	V / =	W / 2	X / /	Y / 6	Z / +	CARRIAGE RETURN	LINE FEED	LETTERS	FIGURES	SPACE	ALL SIGNALS NOT USED
CODE ELEMENTS 1	●	●		●	●	●				●	●						●				●		●	●	●	●			●	●		
2	●		●				●		●	●	●	●				●	●	●			●	●	●					●	●	●		
3			●			●		●	●		●			●		●	●		●		●	●		●	●				●		●	
4		●	●	●			●			●	●		●	●	●			●				●		●			●			●	●		
5		●					●	●				●	●			●	●	●		●		●	●	●	●	●			●	●		

- **Veikimo principas:** Lorenz šifras naudojo 12 rotorių, kurie generuodavo pseudo-atsitiktinę simbolių seką. Ši seka buvo naudojama šifruojamam tekstui modifikuoti, pridedant ją prie originalaus teksto simbolių.
- **Sudėtingumas:** Dėl didesnio rotorių skaičiaus ir sudėtingesnio algoritmo, Lorenz šifras buvo atsparesnis kriptanalizei nei Enigma.



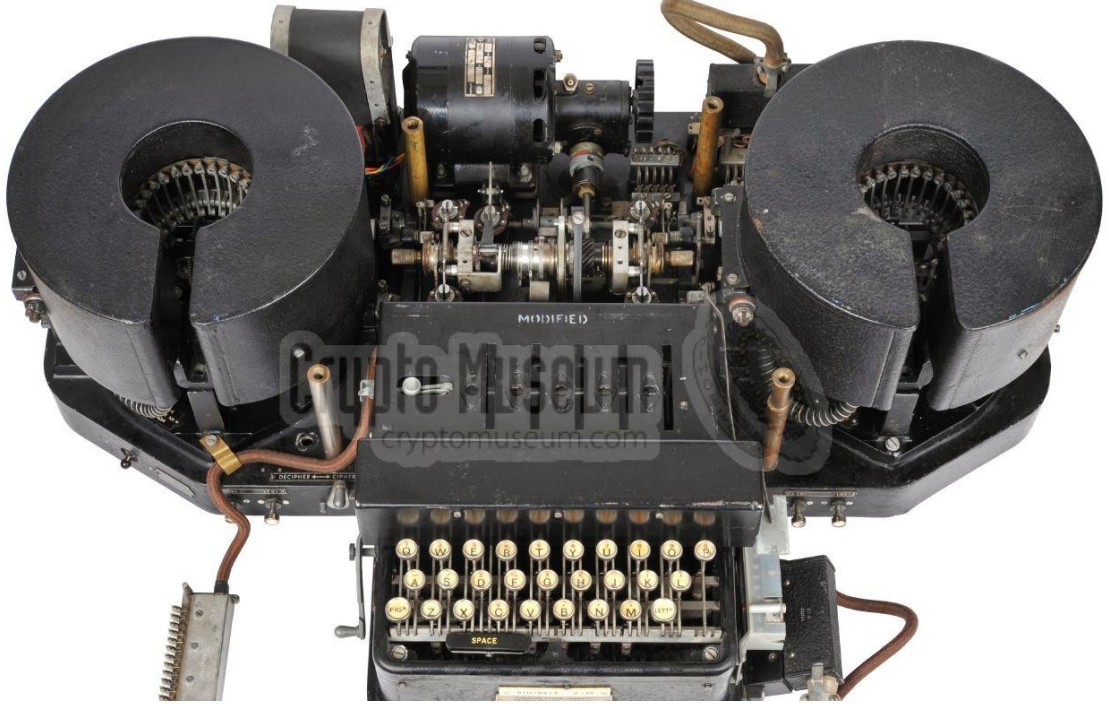
SIGABA

- **Veikimo principas:** SIGABA taip pat naudojo rotorius, bet jų konfigūracija ir tarpusavio sąveika buvo sudėtingesnė nei Enigmoje. Be to, SIGABA turėjo mechanizmus, kurie apsunkino dažnių analizę - vieną iš pagrindinių metodų, naudojamų šiframs laužyti.
- **Saugumas:** Dėl savo sudėtingumo ir unikalių savybių, SIGABA laikoma viena saugiausių Antrojo pasaulinio karo šifravimo mašinų. Manoma, kad jos kodas nebuvo nulaužtas.



Typex

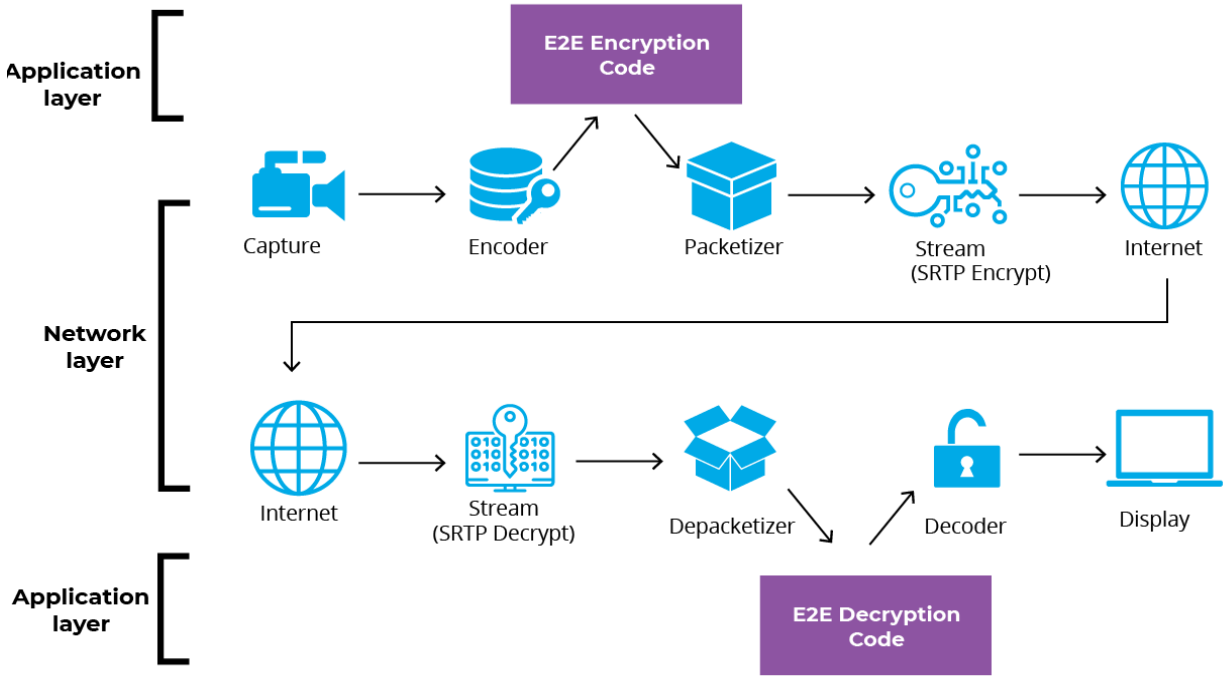
- **Veikimo principas:** Typex buvo panaši į Enigmą, bet turėjo keletą patobulinimų, pavyzdžiui, daugiau rotorių ir spausdinimo mechanizmą.
- **Saugumas:** Nors Typex nebuvo tokia sudėtinga kaip SIGABA, ji vis tiek buvo gana saugi ir plačiai naudojama Britų kariuomenės.



Šiuolaikinis šifravimas ir jo taikymas

Šiuolaikinio šifravimo principai:

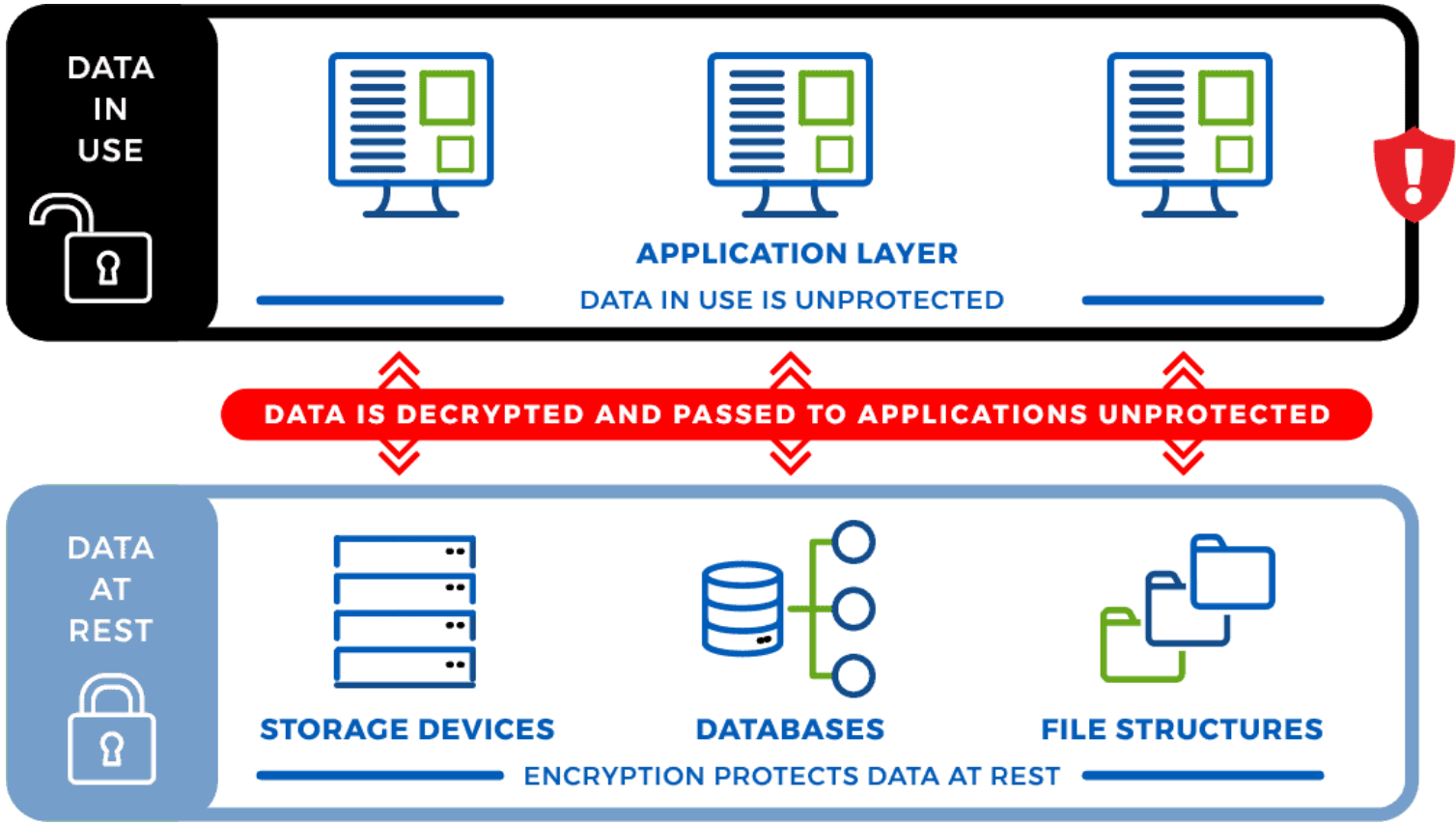
- **Matematinis pagrindas:** Šiuolaikinis šifravimas remiasi sudėtingais matematiniais algoritmais ir skaičiavimo problemomis, kurias sunku išspręsti be rakto.
- **Rakto svarba:** Šifravimo stiprumas priklauso nuo rakto ilgio ir sudėtingumo. Kuo ilgesnis ir sudėtingesnis raktas, tuo sunkiau jį nulaužti.
- **Simetrinis ir asimetrinis šifravimas:** Šiuolaikiniai šifravimo metodai apima ir simetrinį (tas pats raktas šifravimui ir dešifravimui), ir asimetrinį (skirtingi raktai) šifravimą.



Šiuolaikinis šifravimas ir jo taikymas

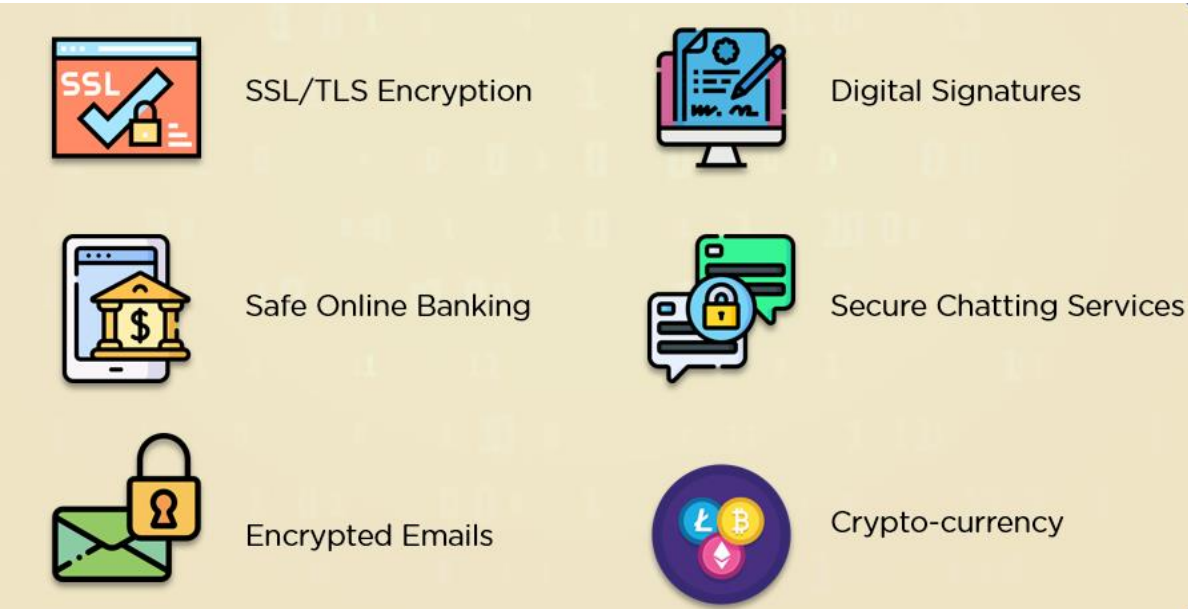
Šifravimo taikymas:

- Šifravimas yra esminis **interneto saugumo** elementas. Jis naudojamas apsaugoti:
  - **Slaptažodžius:** Šifravimas apsaugo slaptažodžius nuo neteisėtos prieigos.
  - **Elektroninius laiškus:** Šifravimas užtikrina, kad tik siuntėjas ir gavėjas galėtų perskaityti el. laiškus.
  - **Finansines operacijas:** Šifravimas apsaugo banko sąskaitas ir internetinius mokėjimus.
  - **Asmens duomenis:** Šifravimas padeda apsaugoti asmens duomenis nuo vagysčių ir piktnaudžiavimo.



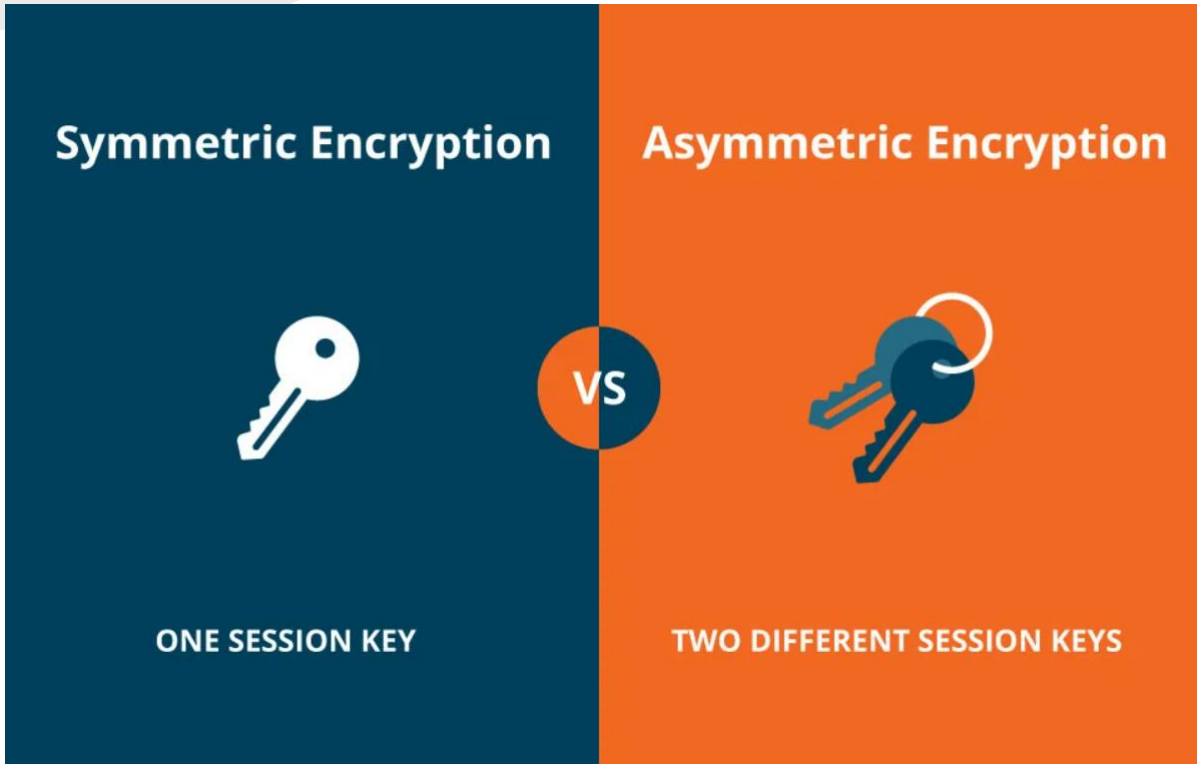
Šiuolaikinis šifravimas ir jo taikymas

- Šifravimas naudojamas **apsaugoti duomenis**, saugomus kompiuteriuose, telefonuose ir kituose įrenginiuose.
- Šifravimas naudojamas **elektroniniams parašams** kurti, kurie užtikrina dokumentų autentiškumą ir vientisumą.
- Šifravimas taip pat naudojamas **daugelyje kitų sričių**, pavyzdžiui, sveikatos apsaugoje (pacientų duomenų apsaugai), vyriausybėje (slaptos informacijos apsaugai), kariuomenėje (ryšių apsaugai).



Šifravimo tipai

- **Simetrinis šifravimas** (tas pats raktas naudojamas šifravimui ir dešifravimui).
- **Asimetrinis šifravimas** (skirtingi raktai naudojami šifravimui ir dešifravimui).

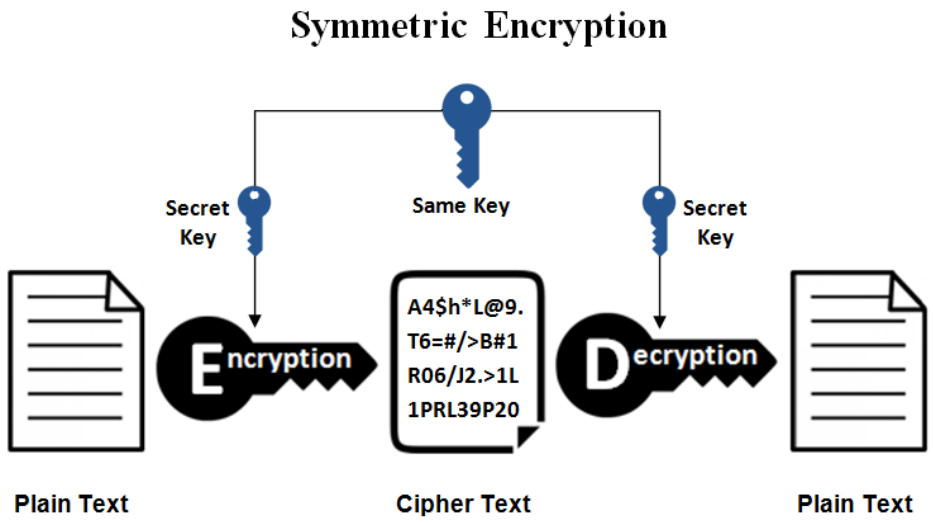


Simetrinis šifravimas

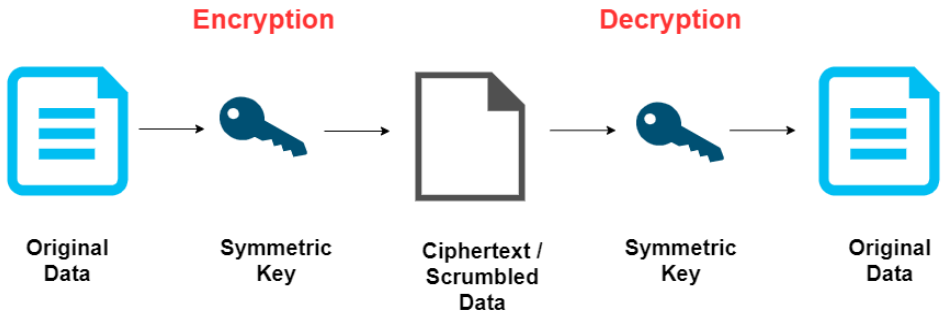
Veikimo principas:

- **Tas pats raktas:** Simetriniame šifravime tas pats raktas naudojamas ir duomenims užšifruoti, ir jiems iššifruoti.

Analogija: Įsivaizduokite, kad turite dėžutę su spyna. Jūs ir jūsų draugas turite vienodus raktus nuo tos spynos. Jūs galite įdėti žinutę į dėžutę, užrakinti ją savo raktu ir išsiųsti draugui. Draugas, naudodamas savo raktą, gali atrakinti dėžutę ir perskaityti žinutę.



Simetrinis šifravimas

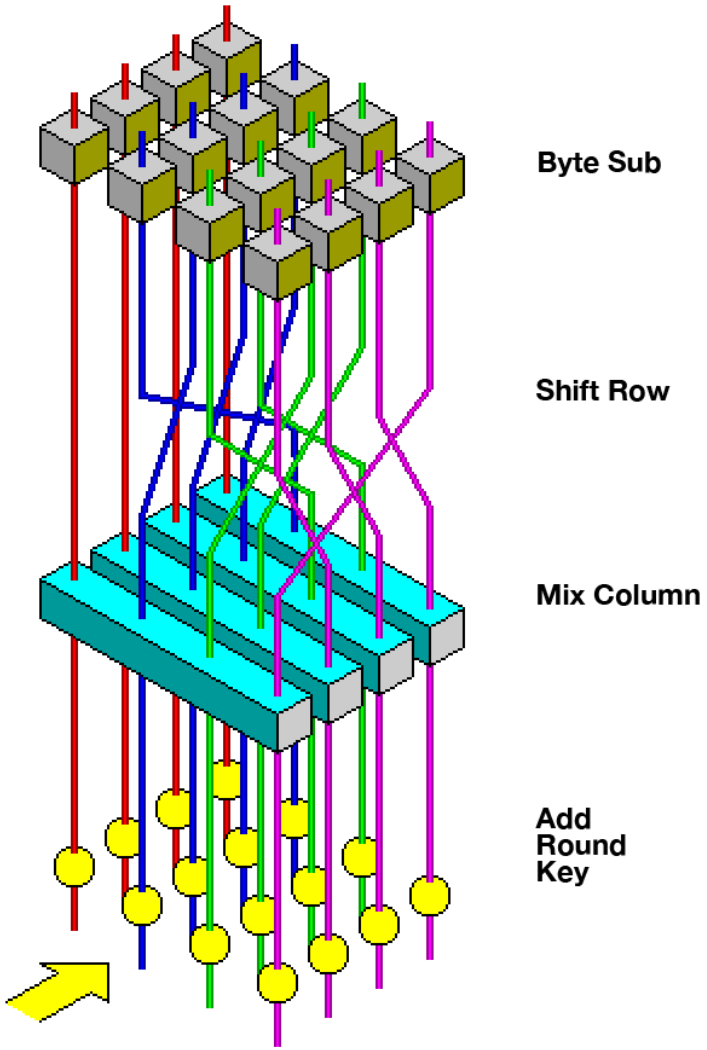


Privalumai

- **Greitis:** Simetrinis šifravimas yra greitesnis ir reikalauja mažiau skaičiavimo resursų nei asimetrinis šifravimas.
- **Paprastumas:** Simetrinio šifravimo algoritmai paprastai yra paprastesni ir lengviau įgyvendinami.

Trūkumai

- **Rakto perdavimas:** Didžiausias simetrinio šifravimo iššūkis yra saugus rakto perdavimas tarp siuntėjo ir gavėjo. Jei raktas patenka į netinkamas rankas, užšifruoti duomenys gali būti lengvai iššifruoti.
- **Rakto valdymas:** Kai bendraujama su daugeliu žmonių, reikia valdyti daug raktų, o tai gali būti sudėtinga.

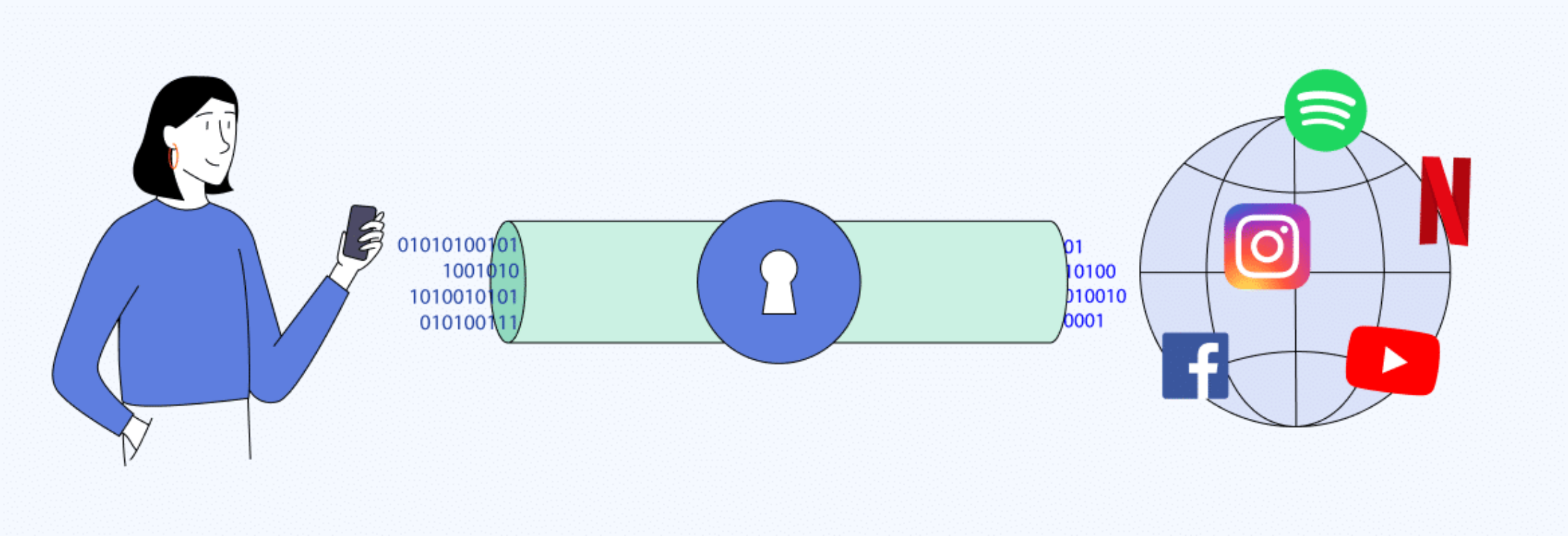


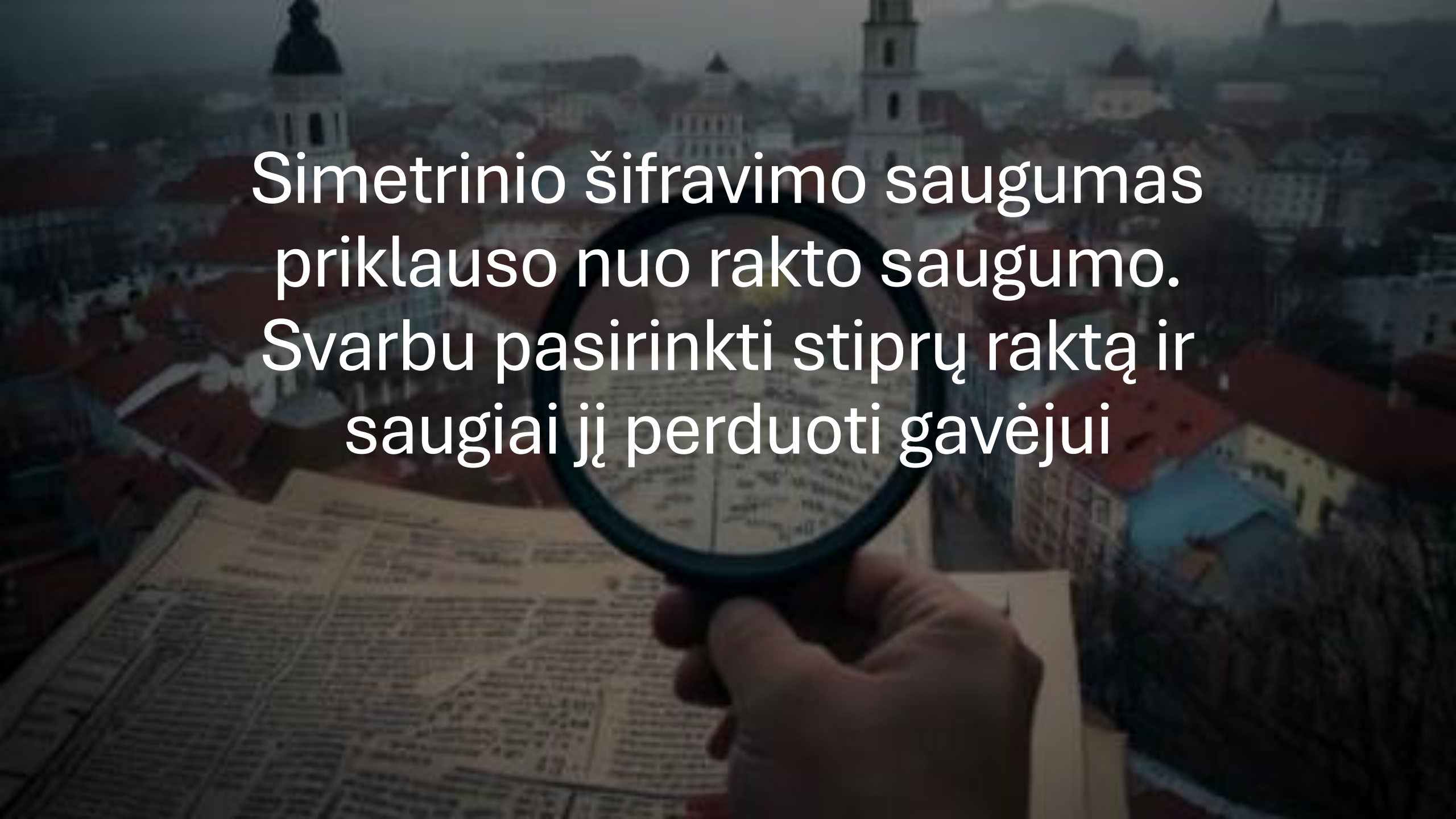
Pavyzdžiai

- **DES (Data Encryption Standard):** Anksčiau plačiai naudotas simetrinio šifravimo standartas, dabar laikomas pasenusiu.
- **AES (Advanced Encryption Standard):** Dabartinis simetrinio šifravimo standartas, plačiai naudojamas įvairiose srityse.
- **Blowfish, Twofish, Serpent:** Kiti simetrinio šifravimo algoritmai.

Taikymas

- **Failų šifravimas:** Apsaugoti failus nuo neteisėtos prieigos.
- **Duomenų bazių šifravimas:** Apsaugoti duomenis, saugomus duomenų bazėse.
- **VPN (Virtual Private Network):** Sukurti saugų ryšį tarp kompiuterių per internetą.
- **Wi-Fi saugumas:** Apsaugoti belaidžius tinklus nuo neteisėtos prieigos.

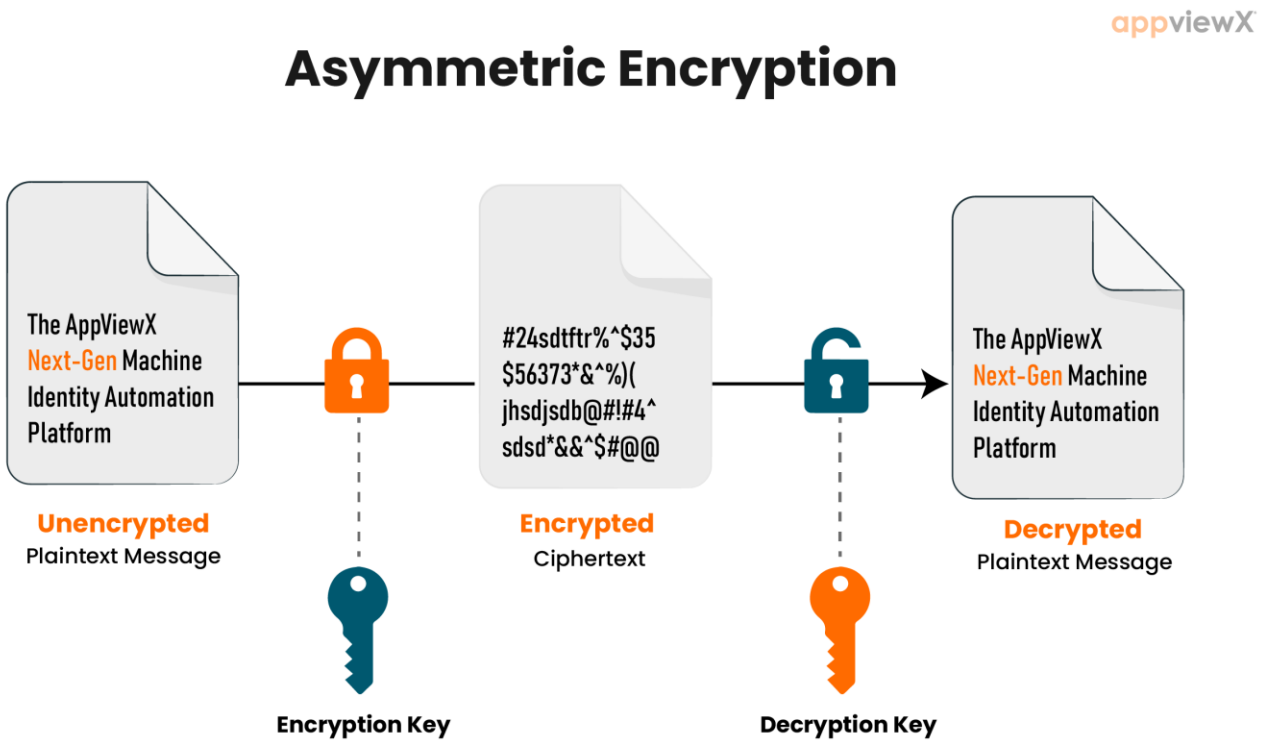




Simetrinio šifravimo saugumas priklauso nuo rakto saugumo. Svarbu pasirinkti stiprų raktą ir saugiai jį perduoti gavėjui

Asimetrinis šifravimas

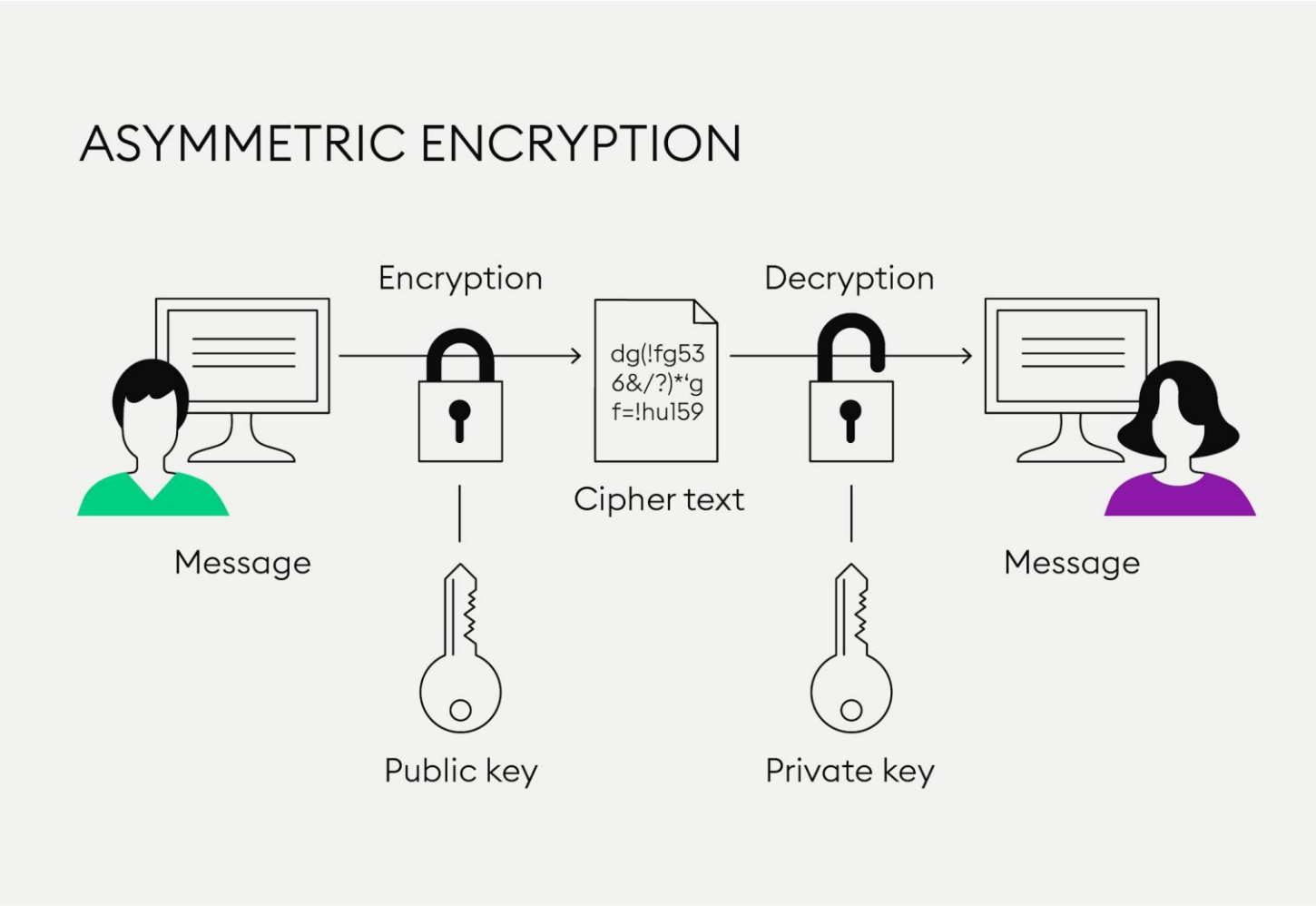
Asimetrinis šifravimas, dar vadinamas viešojo rakto kriptografija, yra šifravimo tipas, kuris naudoja du raktus: **viešąjį raktą** ir **privatųjį raktą**.



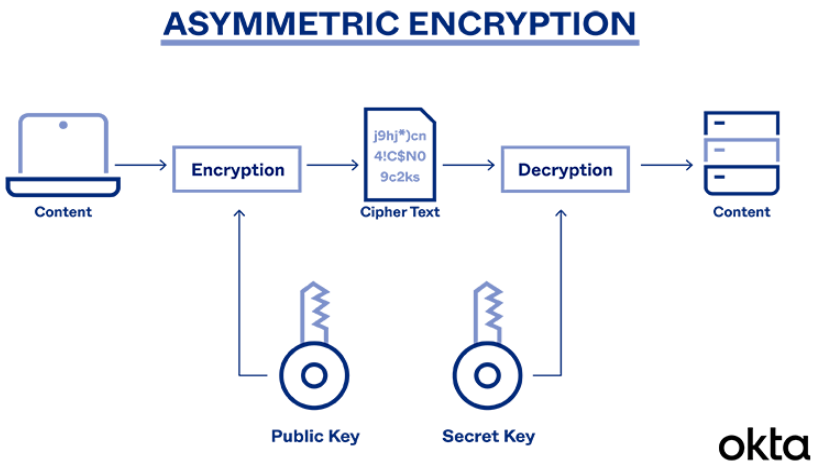
Asimetrinis šifravimas

Veikimo principas:

- **Viešasis raktas:** skirtas duomenims užšifruoti. Jį gali turėti bet kas.
- **Privatusis raktas:** skirtas duomenims iššifruoti. Jį turi tik gavėjas.
- **Analogija:** Įsivaizduokite, kad turite pašto dėžutę su dviem angomis. Viena anga yra atvira visiems (viešasis raktas) - per ją bet kas gali įmesti laišką. Kita anga yra užrakinta (privatusis raktas), ir tik jūs turite raktą ją atrakinti.



Asimetrinis šifravimas



Privalumai

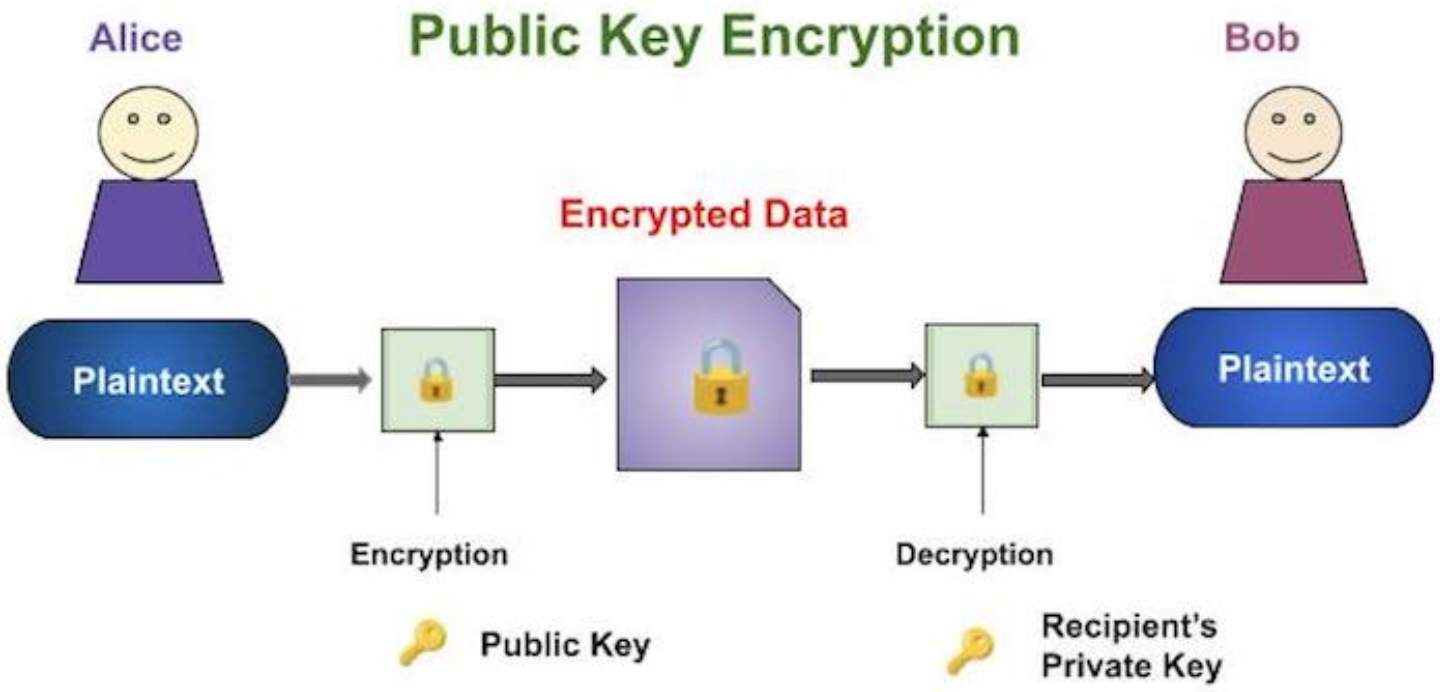
- **Saugus rakto perdavimas:** Nereikia saugiai perduoti rakto tarp siuntėjo ir gavėjo, nes viešasis raktas gali būti viešai prieinamas.
- **Autentifikavimas:** Asimetrinis šifravimas gali būti naudojamas autentifikuoti siuntėją ir užtikrinti, kad žinutė nebuvo pakeista.

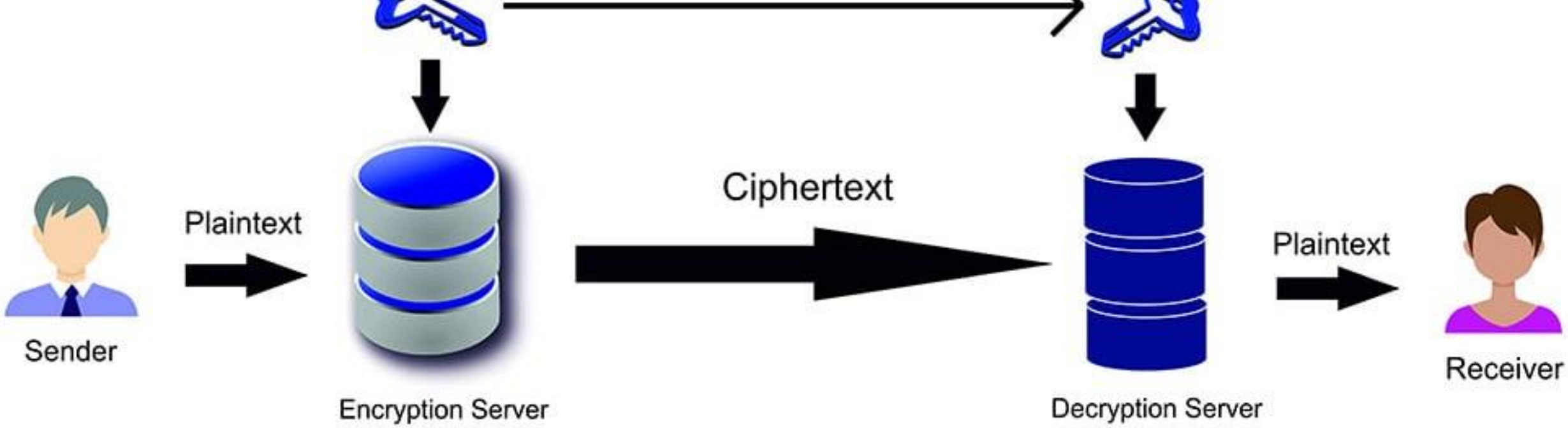
Trūkumai

- **Greitis:** Asimetrinis šifravimas yra lėtesnis nei simetrinis šifravimas.
- **Sudėtingumas:** Asimetrinio šifravimo algoritmai yra sudėtingesni ir reikalauja daugiau skaičiavimo resursų.

Pavyzdžiai

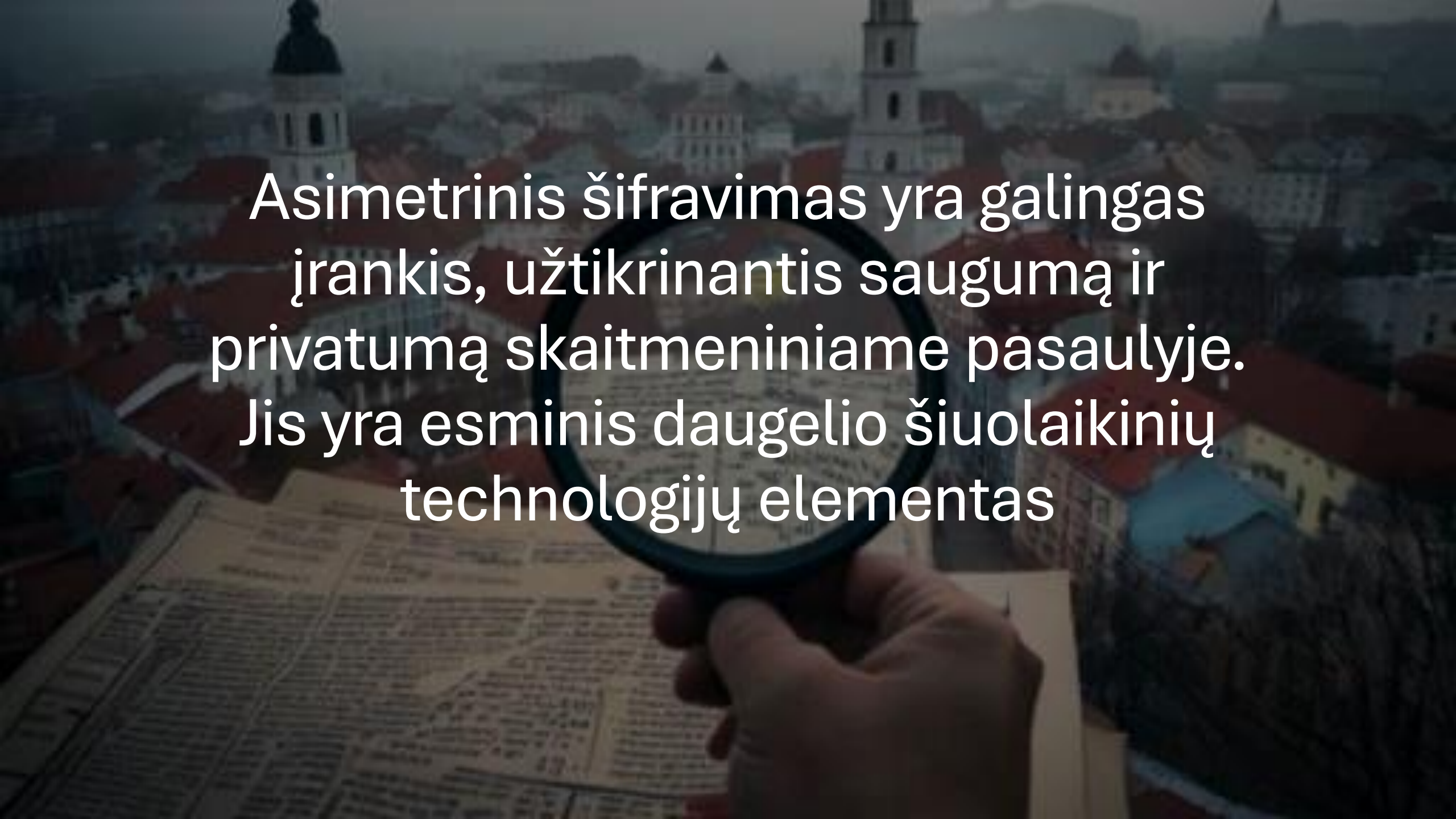
- **RSA:** Plačiai naudojamas asimetrinio šifravimo algoritmas.
- **ECC (Elliptic Curve Cryptography):** Palyginti naujas asimetrinio šifravimo algoritmas, kuris yra efektyvesnis už RSA.





Taikymas

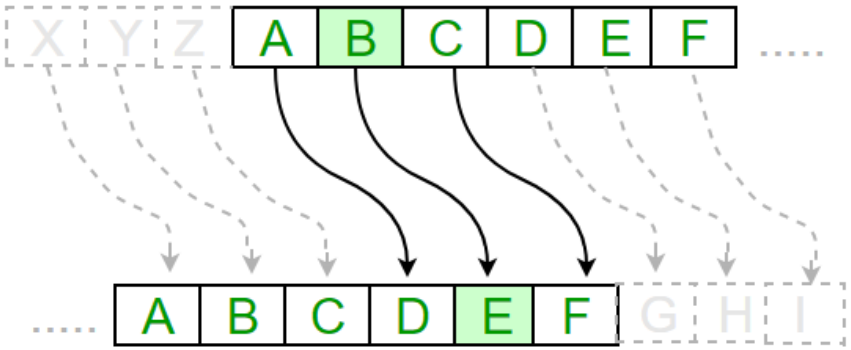
- Asimetrinis šifravimas yra plačiai naudojamas įvairiose srityse, pavyzdžiui:
- **Elektroninis parašas:** Užtikrinti dokumentų autentiškumą ir vientisumą.
- **SSL/TLS sertifikatai:** Apsaugoti interneto ryšius (pvz., https svetainėse).
- **Šifruotas el. paštas:** Užtikrinti, kad tik gavėjas galėtų perskaityti el. laišką.
- **Kriptovaliutos:** Užtikrinti saugius sandorius ir valdyti skaitmeninį turtą.



Asimetrinis šifravimas yra galingas įrankis, užtikrinantis saugumą ir privatumą skaitmeniniame pasaulyje. Jis yra esminis daugelio šiuolaikinių technologijų elementas

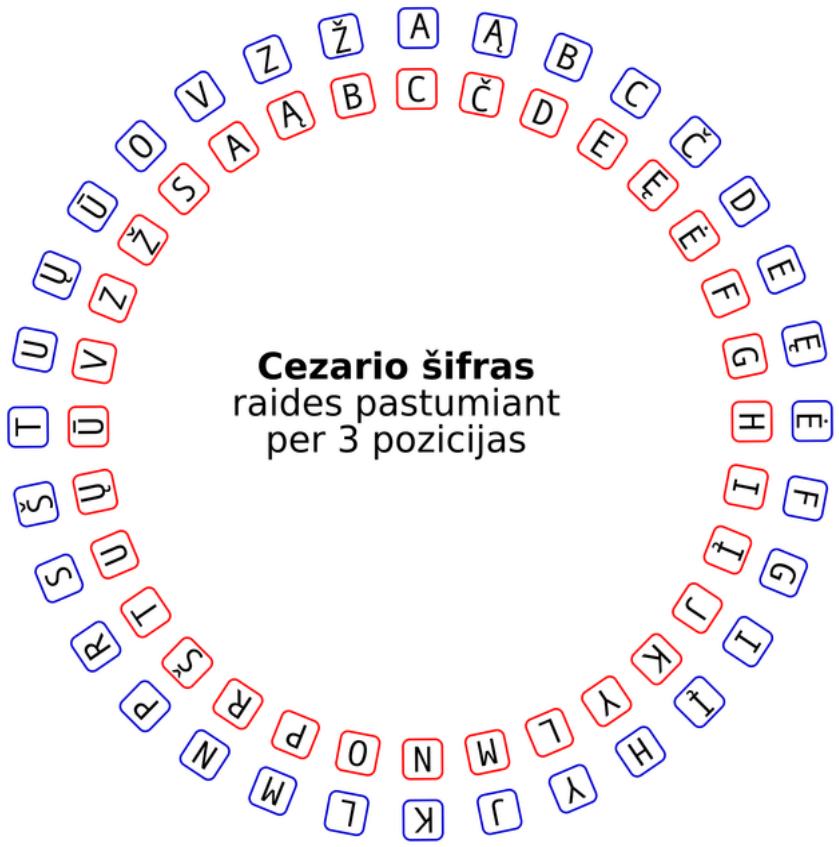
Cezario šifras - paprasta, bet efektyvu!

Raidžių perkėlimas per fiksuotą pozicijų skaičių.



Cezario šifras

Cezario šifras yra vienas iš seniausių ir paprasčiausių šifravimo metodų, pavadintas Romos imperatoriaus Julijaus Cezario vardu, kuris jį naudojo savo karinėje korespondencijoje.



K A M U O L I U K A S
N C P V S O J V N C U

P A S L Ė P T A S
Š C U O H Š Ū C U

K R Ū M U O S E
N T Ž P V S U F

Veikimo principas

Cezario šifras veikia perkeliant kiekvieną teksto raidę per fiksuotą pozicijų skaičių abėcėlėje. Šis fiksuotas skaičius yra šifro raktas. Pavyzdžiui, jei raktas yra 3, raidė "A" būtų pakeista raide "D", raidė "B" - raide "E" ir taip toliau.

https://skaiciuotuvai.lt/cezario-sifras-internetinis-kodavimo-dekoderis

Pavyzdys

Tekstas: Vilnius

Raktas: 11

Užšifruotas tekstas: Gtwytfd

Dešifravimas:

Norint iššifruoti tekstą, užkoduotą Cezario šifru, reikia perkelti kiekvieną raidę atgal per rakte nurodytą pozicijų skaičių.

Cezario šifras

Privalumai

- **Paprastumas:** Cezario šifras yra labai paprastas suprasti ir naudoti.
- **Greitis:** Šifravimas ir dešifravimas yra greiti procesai.

Trūkumai

- **Nesaugumas:** Cezario šifras yra lengvai nulaužiamas, nes yra tik ribotas skaičius galimų raktų (tiek, kiek raidžių yra abėcėlėje).

Taikymas

Nors Cezario šifras nėra saugus šiuolaikiniais standartais, jis vis dar gali būti naudojamas edukaciniais tikslais arba paprastiems žaidimams ir galvosūkiams kurti.

Variacijos

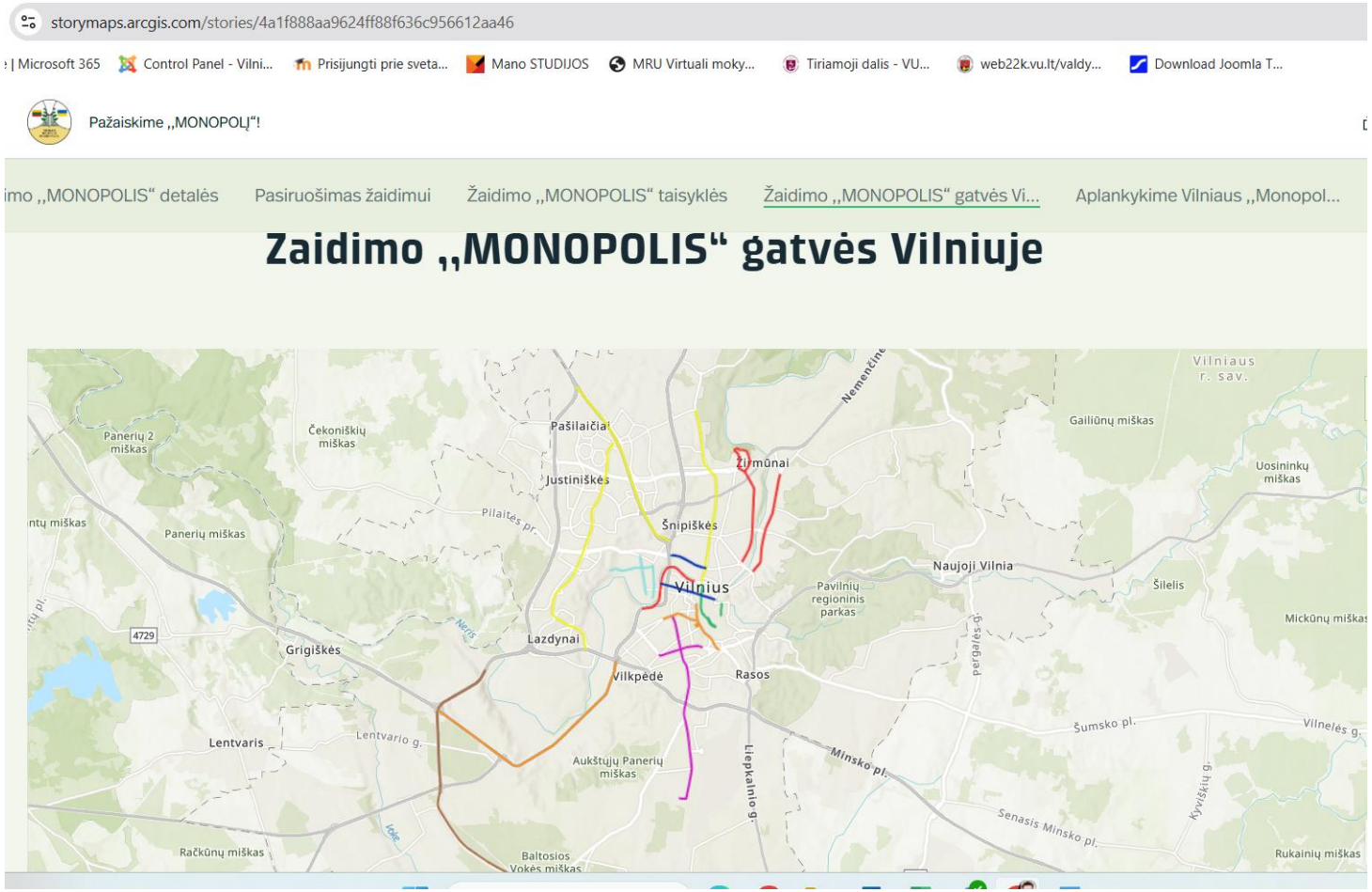
- **ROT13:** Kiekviena raidė perkeliama per 13 pozicijų.
- **Šifras su rakto žodžiu:** Raktas yra žodis, o raidės perkeliamos pagal to žodžio raidžių pozicijas abėcėlėje.

Įdomybės

- Cezario šifras yra monoalfabetinio pakeitimo šifro pavyzdys.
- Jis gali būti lengvai nulaužtas naudojant dažnių analizę.

Geolokacinės istorijos

- Pasakojimas, susietas su konkrečiomis geografinėmis vietomis.
- **Platformos:** Google Earth, StoryMapJS, ArcGIS StoryMaps.



Užduoties pristatymas

Iššifruokite Vilniaus paslaptis!

Instrukcijos

1. Gausite užduočių lapą su 5 užkoduotomis Vilniaus vietomis (Cezario šifras, be rakto).
2. Iššifruokite vietų Vilniuje pavadinimus.
3. Raskite šias vietas Google Earth, pažymėkite jas ir pėsčiomis nuvykite iki jų. Šifruotėje bus aprašyta, kokio objekto nuotrauką toje vietoje Jūs turite padaryti.
4. Nufotografuokite kiekvieną iš 5 objektų ir įkelkite nuotraukas į Google Earth su trumpu aprašymu.
5. Klasėje sukurkite geolokacinę istoriją, įpindami istorinių faktų apie aplankytas vietas.

Vienybė - jėga!

Komandinis darbas

Bendradarbiavimas

Idėjų dalinimąsis

Užduoties tikslas

Taikydami Cezario šifro dekodavimo principus, turite iššifruoti objektų pavadinimus ir, pasinaudodami Google Earth programėle bei kitais informacijos šaltiniais, surasti šiuos objektus Vilniaus senamiestyje.

Darbo lapas, pateiktas žemiau, naudoja vieną iš pateikiamų 5 lankytinų vietų. Raudonai pažymėti objektai užkoduoti su raktu, lygiu Gedimino stulpų skaičiui

Grupė: Data:

Iššifruok Vilniaus kodą

Darbo lapas

Cezario šifro raktas yra Gedimino stulpų skaičius

1.Ką turite rasti ir nufotografuoti:

Urwxšėv dlnšwėv vnxoswūud

Pastaba apie objektą

Trumpai pažymėkite, ką reikia įtraukti į geolokacinę istoriją

2. Ką turite rasti ir nufotografuoti:

Yloqldxv Ndwhgurv ylwudždv

Pastaba apie objektą

Trumpai pažymėkite, ką reikia įtraukti į geolokacinę istoriją

3. Ką turite rasti ir nufotografuoti:

Jhglplqr ndoqr sdqrudpd

Pastaba apie objektą

Trumpai pažymėkite, ką reikia įtraukti į geolokacinę istoriją

Grupė: Data:

Iššifruok Vilniaus kodą

Darbo lapas

Cezario šifro raktas yra Gedimino stulpų skaičius

4. Ką turite rasti ir nufotografuoti:

Yloqldxv xqlyhuvlwhwr dxglwrulmd

Pastaba apie objektą

Trumpai pažymėkite, ką reikia įtraukti į geolokacinę istoriją

5. Ką turite rasti ir nufotografuoti:

Yloqldxv vhqdplhvčlr jdwyėv sdydglqlpdv

Pastaba apie objektą

Trumpai pažymėkite, ką reikia įtraukti į geolokacinę istoriją

Laukiame įdomių atradimų!

Sėkmės!