Simetrinis ir asimetrinis šifravimas, kriptografinės sistemos

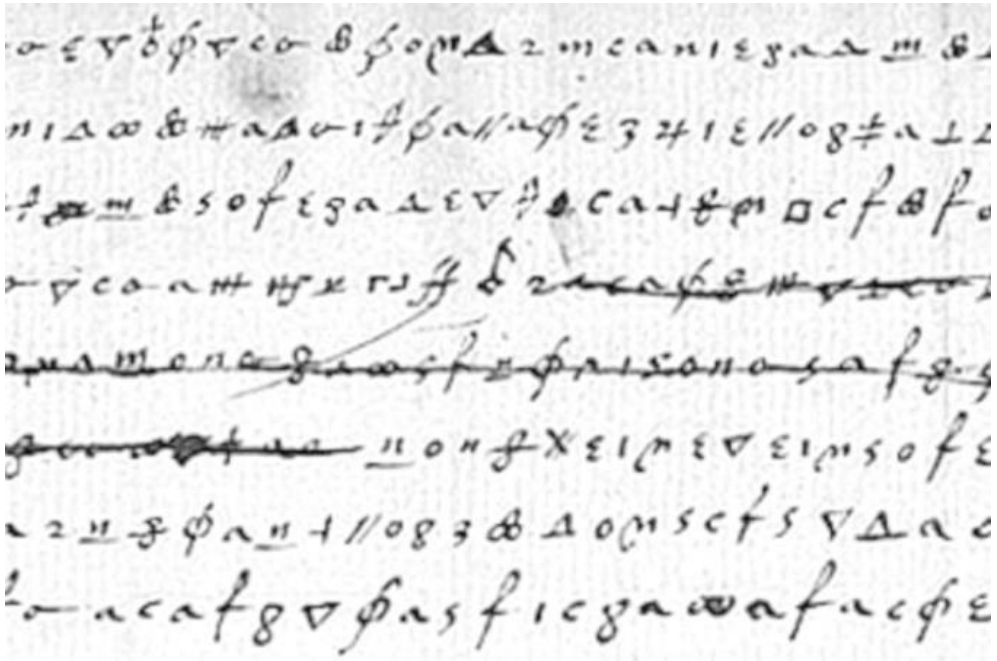
Mokytoja V. Bernotienė

Pranešimų šifravimas

- Žmonės visada ieškojo būdų saugiai perduoti informaciją.
- Šifravimo raidą lėmė ir lemia besitęsianti kova tarp **šifro kūrėjų** ir siekiančių atskleisti šifro raktą (kartais vadinamų **„šifro laužytojų“**).

Sąvokos:

- **Paprastas tekstas** yra pranešimas prieš šifravimą.
- **Šifruotas tekstas** yra pranešimas po šifravimo.
- **Žodžiai *iššifravimas* ir *dešifravimas* yra sinonimai.**



Užšifruoto laiško, susijusių su M. Stiuart istorija, fragmentas (Kodų kūrėjų ir jų laužytojų kova susijusi ir su garsiausių karališkųjų šeimų intrigomis (lrytas.lt))

Klasikinis pavyzdys apie šifruoto teksto svarbą yra 16 amžiuje Škotijos karalienės Marijos Stiuart, rengusios sąmokslą prieš Anglijos karalienę Elžbietą I ir siekusios užimti Anglijos karalienės sostą, istorija. Ji buvo įkalinta, bet ilgą laiką trūko įrodymų dėl jos kaltės. Viena iš pagrindinių ilgo įkalinimo priežasčių buvo sunkumai iššifruoti sąmokslo dalyvių užšifruotus laiškus. Tie šifruoti laiškai vėliau buvo pavadinti *„Babingtono laiškais“* (*Babingtonas* – vienas iš sąmokslo dalyvių). Pagaliau Elžbietos I slaptojoje tarnyboje laiškai buvo iššifruoti. Jų turinys lėmė, kad Marija Stiuart buvo teisiama dėl sąmokslo ir vėliau jai buvo įvykdyta mirties bausmė. Tai buvo ne pirmas kartas istorijoje, kai žmogaus gyvenimas ar visos valstybės likimas priklausė nuo šifro jėgos.

Kriptografinių sistemų apibūdinimas (1)

- **Kriptografija** – iš graikų kalbos ***kripto*** *(paslėptas)* ir ***grafos*** *(rašymas)*.
- Kriptografija reiškia paslėptą rašymą, kurio **tikslas** aiškus – taip norima **apsaugoti informaciją** ir neleisti trečiosioms šalims prie jos prieiti.
- **Kriptografinės sistemos** – tai matematikos ir informatikos disciplinos, kurioje nagrinėjami duomenų užšifravimo ir šifro atkūrimo (iššifravimo) metodai.
- **Jų tikslas – užtikrinti informacijos saugumą nuo nepageidaujamų asmenų** (nuo asmenų, kurie neturi teisės matyti ar modifikuoti šiuos duomenis).

Kriptografinių sistemų apibūdinimas (2)

- **Kriptografijos istorija** apima daugiau nei **4000 metų**. Istorinės kriptografinės sistemos yra labai svarbios metodologine pažintine prasme (keletą aptarsime).

Užduotis pamąstymui ir diskusijai

Brangius daiktus, svarbią informaciją įstaigos, žmonės dažnai laiko seifuose. Kodėl, jūsų manymu, informacijos apsaugai nepakanka seifų, kodėl reikia sudėtingų kriptografinių sistemų (šifravimo)?

Šifravimo tikslai

- **Šifravimo tikslai** – tai ilgalaikės kryptys arba bendrosios vizijos, kurias norima pasiekti per informacijos šifravimą.
- Vienas pagrindinių šifravimo tikslų – **užtikrinti duomenų konfidencialumą (saugumą)**. Tai siekis sutrukdyti pašaliniams asmenims susipažinti su slapta informacija.
- Kitas tikslas gali būti **užtikrinti duomenų integralumą (vientisumą)** – garantuoti, kad duomenys nebuvo pakeisti neleistinai.

Šifravimo uždaviniai

- **Šifravimo uždaviniai** – tai priemonės įveikti konkrečioms problemoms ar kliūtims siekiant ilgalaikių tikslų.

- Pavyzdžiui, jei tikslas yra **„Užtikrinti duomenų konfidencialumą“**, tai vienas iš uždavinių gali būti **„Sukurti šifravimo algoritmą, kuris būtų atsparus „nulaužimui“**. Kitas uždavinys gali būti **„Sukurti saugų būdą rakto perdavimui tarp siuntėjo ir gavėjo“**.

Kalbant apie šifravimą, ***tikslai dažnai yra susiję su duomenų saugumu***, o ***uždaviniai yra techninės ar praktinės priemonės***, susijusios su šių tikslų įgyvendinimu.

Duomenų šifravimas (1)

Šifravimas – tai būdas saugoti mūsų duomenis, informaciją, žinutes nuo „smalsių akių“:

- vaikams tai gali būti įdomiu žaidimu;
- suaugusiems ir įmonėms bei organizacijoms tai būdas apsaugoti svarbią informaciją ir pranešimus nuo tų, kurie neturi (ar jiems nebūtina) šios informacijos žinoti.

Duomenų šifravimas (2)

- **Šifravimo raktai** – konkrečios šifravimo taisyklės, schemos, metodai.
- **Šifravimo raktas yra informacija, kuri nustato, kaip pradinis tekstas bus pakeistas šifruotu tekstu.**
- Tai gali būti raidžių keitimo kitomis raidėmis ar konkrečiais simboliais, įvairios schemos, būdai ar gana sudėtingos matematiniais metodais pagrįstos procedūros.
- Šifravimo raktą būtina **laikyti saugiai**. Jei kas nors sužinos šifravimo raktą, jis galės iššifruoti šifruotą tekstą.

Kriptografijos tipai

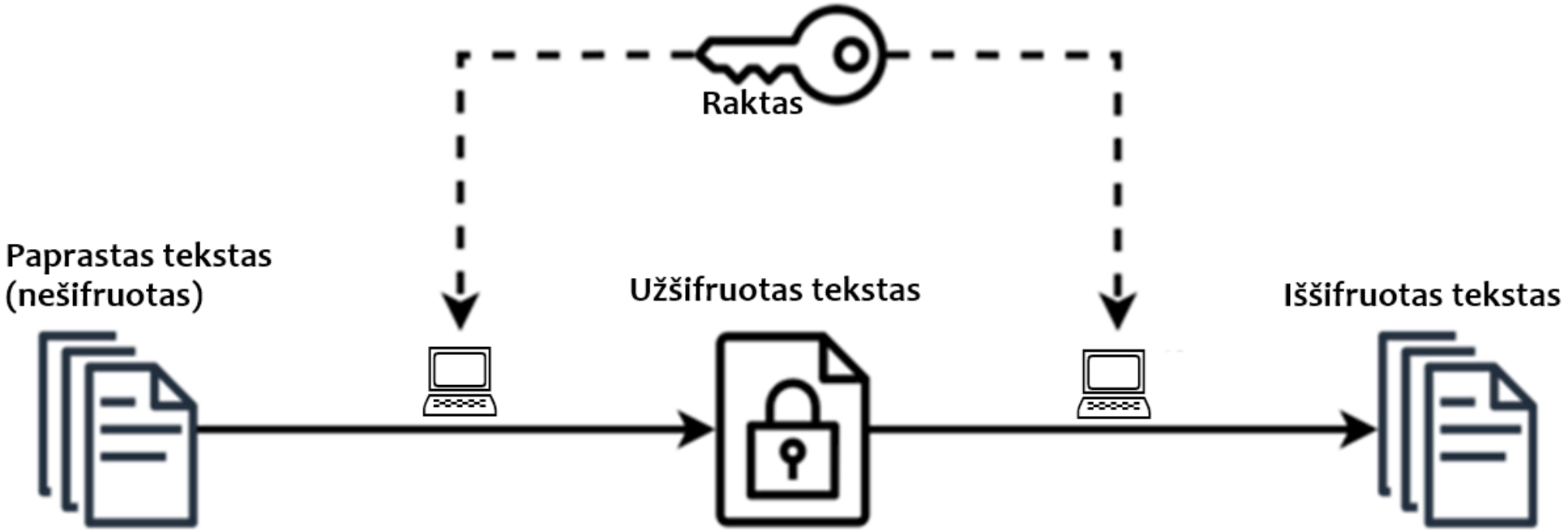
- **Simetrinė kriptografija –** tai kriptografijos tipas, kai **tie patys šifravimo raktai** naudojami tiek užšifravimui, tiek iššifravimui. Taip šifruojant, pranešimo siuntėjas ir gavėjas turi turėti tą patį raktą, kad užšifruotas pranešimas būtų perskaitytas.
- **Asimetrinėje kriptografijoje –** pranešimo užšifravimui ir iššifravimui šiame **naudojami skirtingi raktai**. Paprastai yra ***viešasis raktas***, kuris yra prieinamas visiems ir naudojamas užšifravimui, bei ***privatūs raktai***, kurie naudojami tik iššifravimui ir yra laikomi paslaptyje.
- **Hibridinė kriptografija** kombinuoja simetrinės ir asimetrinės kriptografijos privalumus. Paprastai naudojama asimetrinė kriptografija saugiam simetrinio rakto perdavimui, o po to su šiuo simetriniu raktu šifruojami duomenys.

Simetrinė kriptografija gali būti skirstoma

- **Šifravimas nenaudojant kompiuterių** – dažniausiai yra istoriniai šifravimo metodai, kurie buvo naudojami prieš kompiuterių erą, pavyzdžiui, *Cezario šifras*, *Skytale*, *Knyginis šifras*, *Perstatų šifras* ir kt.

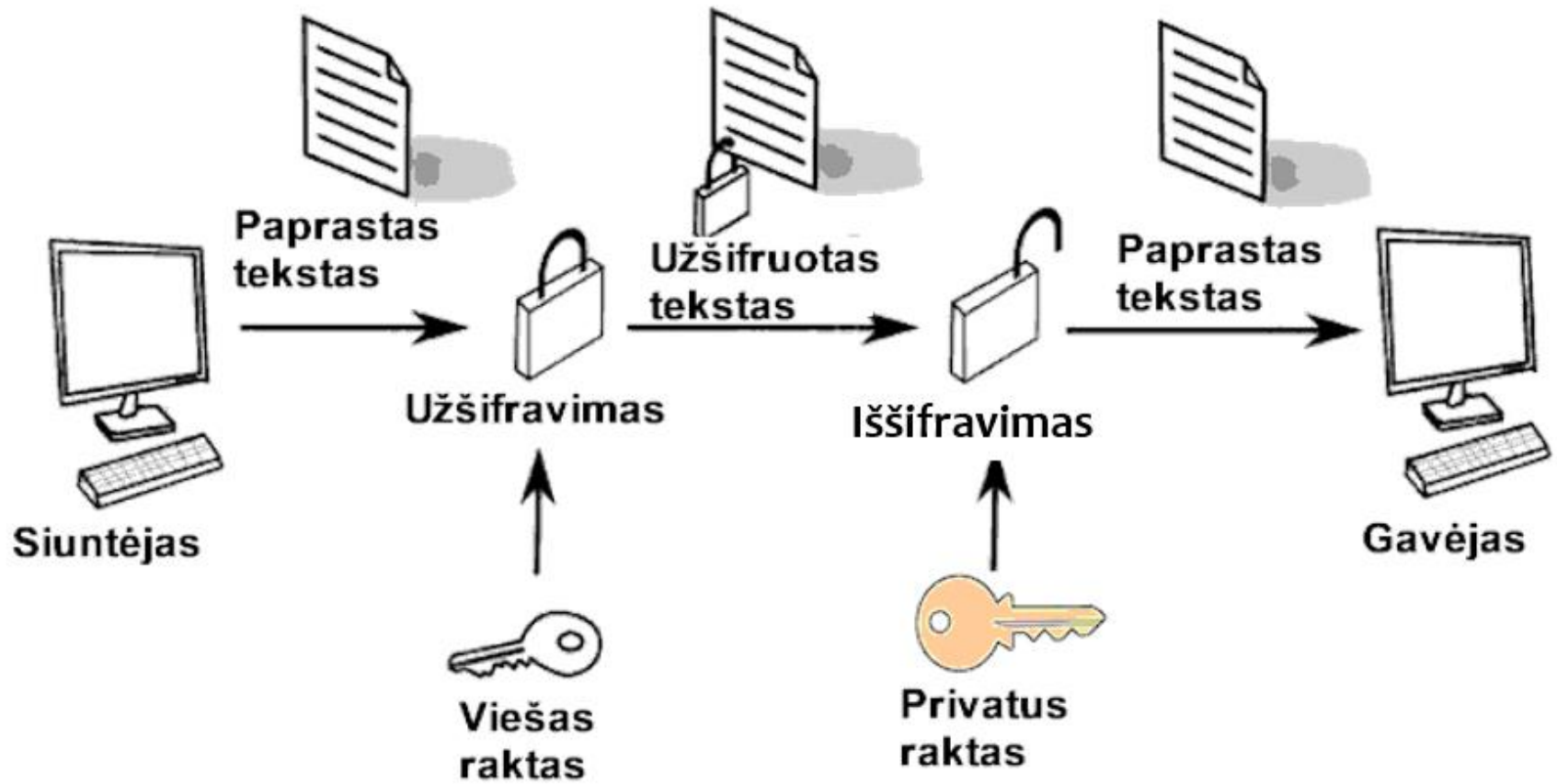
- **Šifravimas naudojant kompiuterius**, pavyzdžiui, *Advanced Encryption Standard* (*AES – Išplėstinis šifravimo standartas*), kuris yra vienas iš populiariausių ir plačiausiai naudojamų simetrinio šifravimo algoritmų.

Simetrinio šifravimo naudojant kompiuterius schema



Naudojimas

- **Simetrinių kriptografinių sistemų naudojimo pavyzdžiai:**
  - duomenų saugojimas,
  - komunikacija,
  - automobilių pramonė,
  - medicinos įrenginiai,
  - tinklų saugumas,
  - elektroninė prekyba,
  - virtualūs privatūs tinklai (VPT),
  - ir kt.


Paprastas tekstas
Užšifruotas tekstas
Paprastas tekstas
Siuntėjas
Užšifravimas
Iššifravimas
Gavėjas
Viešas raktas
Privatus raktas

Naudojimas

- **Asimetrinių kriptografinių sistemų naudojimo pavyzdžiai:**
  - duomenų saugojimas,
  - komunikacija,
  - interneto saugumas,
  - tinklo technologijos,
  - VPT (virtualūs privatūs tinklai),
  - elektroniniai laiškai ir komunikacija,
  - skaitmeniniai parašai,
  - e. dokumentų patvirtinimas,
  - finansinės paslaugos,
  - ir kt.

Kurį pasirinkti?

- Simetrinis šifravimas yra greitas ir paprastas, bet kyla problemų, kai reikia saugiai pasidalyti ir saugoti raktus.
- Asimetrinis šifravimas šias problemas sprendžia, bet yra lėtesnis ir reikalauja daugiau kompiuterio resursų.

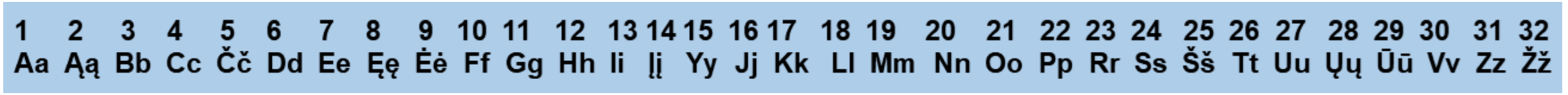
Simetrinės kriptografijos pavyzdžiai ir užduotys (nenaudojant kompiuterio)

Naudojamas raidžių pakeitimas kitomis raidėmis ar simboliais pagal tam tikras taisykles, schemas arba postūmį per kelias abėcėlės raides. Tokio šifravimo metu rekomenduojama prieš akis turėti abėcėlę, pavyzdžiui, lietuvišką sunumeruotą abėcėlę:

Abėcėlė (tekstas)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Aa	Ąą	Bb	Cc	Čč	Dd	Ee	Ęę	Ėė	Ff	Gg	Hh	Ii	Įį	Yy	Jj	Kk	Ll	Mm	Nn	Oo	Pp	Rr	Ss	Šš	Tt	Uu	Ųų	Ūū	Vv	Zz	Žž

Abėcėlė (paveikslėlis)



Julijaus Cezario šifravimo būdas

Julijaus Cezario šifravimo būdą galima nusakyti labai paprastai:
„Keisk abėcėlės raidę trečiąja jos kaimyne“.

Julijaus Cezario šifras pritaikytas lietuviškai abėcėlei

Pagal Vilių Stakėną

Nors Cezario šifras šiandien yra laikomas gana paprastu ir lengvai atskleidžiamu, jis buvo vienas iš pirmųjų bandymų užtikrinti komunikacijos saugumą. Tai rodo, kad šifravimo svarba buvo suprasta jau seniai, ir tai buvo esminė saugaus komunikavimo dalis istorinių karinių ir politinių operacijų metu.

Užduotis

Laikinai pasijuskite Julijumi Cezariu ir, naudodami šį simetrinio šifravimo būdą, užšifruokite kokią nors jo mintį, pvz. iš https://www.c1.lt/zyme/gajus-julijus-cezaris/, ar kokią nors patarlę ir slaptai perduokite draugui(-ei) perskaityti. Aptarkite šį informacijos šifravimo būdą saugumo aspektu.

Šifravimas naudojant lietuviška numeruotą abėcėlę

Jokūbas su Morta susitarė keistis šifruotais pranešimais, pakeičiant kiekvieną raidę raide, kuri yra abėcėlėje už kelių raidžių. Tos keitimo raidės atstumas (postūmis) nurodomas pirmąja šifruoto pranešimo raide, tiksliau jos numerio skaičiumi, pavyzdžiui Ą reiškia postūmį per 1 raidę, M postūmį per 18 raidžių. Šifruotame tekste, vaikams susitarus, tarpai tarp žodžių ir skyrybos ženklai nenaudojami.

Štai žodžio „SUSITIKIME“ šifruotas žodis – „BUVUJŪJNJPF“.

Užduotis

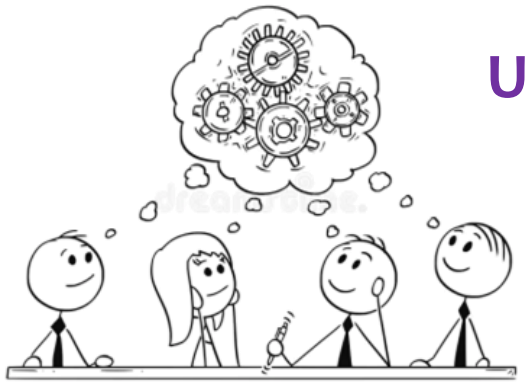
Nustatykite, kokį keičiamos raidės atstumą (postūmį) pasirinko vaikai. Pabandykite šiuo šifravimo metodu užšifruoti savo vardą ar trumpą tekstą. Šifruotais tekstais pasikeiskite su klasės draugais. Pabandykite gautą draugo tekstą iššifruoti.

Šifravimo pavyzdys naudojant raidžių keitimą simboliais pagal pateiktą schemą (raktą)

1. A -> @
2. Ą -> #
3. B -> $
4. C -> %
5. Č -> ^
6. D -> &
7. E -> *
8. Ę -> (
9. Ė ->)
10. F -> -
11. G -> +
12. H -> =
13. I -> <
14. Į -> >
15. Y -> /
16. J -> !
17. K -> 1
18. L -> 2
19. M -> 3
20. N -> 4
21. O -> 5
22. P -> 6
23. R -> 7
24. S -> 8
25. Š -> 9
26. T -> 0
27. U -> :
28. Ų -> ;
29. Ū -> [
30. V ->]
31. Z -> {
32. Ž -> }

Šią informacijos šifravimo schemą (raktą) naudojo Šarūnas ir Živilė. Šis raktas buvo blogai saugomas ir jį aptiko klasės draugas Žilvinas, kartu su šifruotu pranešimu: **,,} <] < 2 * 8 : 8 < 0 < 1 < 3 * $ < $ 2 < 5 0 * 1 5 ! * 9 @ 7 [4 @ 8 “ .**

Naudodamas raktą Žilvinas labai lengvai perskaitė pranešimą ir sužinojo Šarūno ir Živilės paslaptį. Pabandykite šį pranešimą iššifruoti ir jūs.

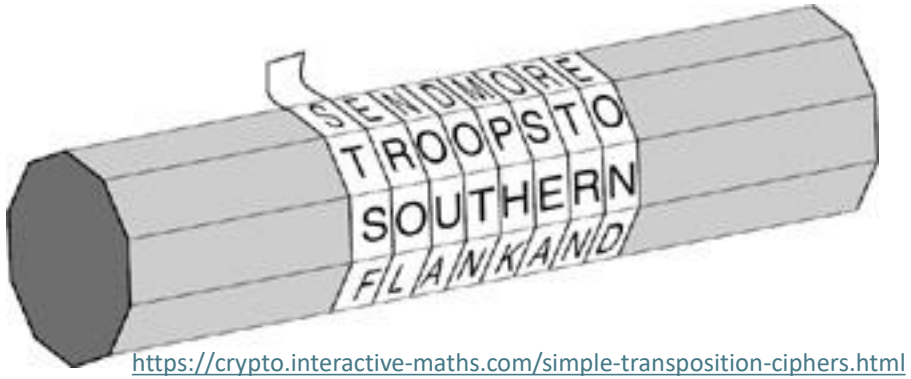


https://www.dreamstime.com/cartoon-business-team-meeting-brainstorming-cartoon-stick-man-drawing-conceptual-illustration-business-team-meeting-image110204670

Užduotis pamąstymui ir diskusijai

Ar garbingai pasielgė Žilvinas perskaitęs aptiktą pranešimą, nors žinojo, kad tai Šarūno ir Živilės slaptas susirašinėjimas. Kaip pasielgtumėte jūs?

Sudėtingesni šifravimo metodai. SKYTALĖ – Spartos šifras



https://crypto.interactive-maths.com/simple-transposition-ciphers.html

Skytalė yra vienas iš seniausių žinomų šifravimo įrankių. Tai mechaninis įrenginys, kurį naudojo senovės graikai, ypač Spartos kariuomenė, norėdami šifruoti pranešimus. Šifro pavadinimas „*skytale*“ kilęs iš graikų žodžio, reiškiančio ritinį, cilindrą arba lazdelę.

Juostelėje užšifruotas pranešimas Spartos kariuomenės vadui (apie 1000 m. pr. m. e.) – siųsti daugiau karių į pietinį mūšio flangą. Atvyniojus juostelę, nenaudojant ritinio, tekstą perskaityti beveik neįmanoma – ypač senovėje, kai buvo mažai raštingų žmonių ir jie apie šifravimą nieko nežinojo arba žinojo mažai.

Pagal Simon Singh

Užduotis

Naudodami paprasto popieriaus lapo juosteles ir jums prieinamas skirtingo skersmens lazdeles užšifruokite trumpą pranešimą spartiečių stiliumi. Pasikeitus juostelėmis, bandykite perskaityti gautą užšifruotą tekstą. Jei kam pavyktų tai padaryti, aptarkite, ką buvo galima padaryti geriau, kad teksto atskleidimas būtų labiau apsunkintas.

Perstatų (perstatymų) šifras

Perstatymo šifras (angl. *transposition cipher*) – tai kriptografijos metodas, kuriame teksto simboliai išdėstomi nauja tvarka, bet nekeičiami į kitus simbolius. Vienas iš labiausiai žinomų perstatymo šifrų pavyzdžių yra **stulpelių perstatymo šifras**.

Pavyzdys su stulpelių perstatymo šifru. Tarkime, turime raktą „3124“ ir tekstą, kurį norime užšifruoti: „ŠIS TEKSTAS YRA SLAPTAS“.

Simbolių Išdėstymas:

Tekstą išdėstome po stulpeliais taip, kaip nurodo raktas. Kiekvienas stulpelis atitinka vieną rakto skaitmenį.

```
3 1 2 4   <-- Šifravimo raktas
-------
Š I S T
E K S T
A S Y R
A S L A
P T A S
```

Perstatymas:

Stulpeliai perstatomi (pakeičiama jų išdėstymo tvarka) – taip gaunamas užšifruotas pranešimas:

```
1 2 3 4
-------
I S Š T
K S E T
S Y A R
S L A A
T A P S
```

Gautas užšifruotas tekstas: „ISŠTKSETSYARSLAATAPS“.

Dešifravimas

Dešifravimas atliekamas atvirkščiai: tekstas yra suskaidytas į stulpelius pagal šifruoto teksto ilgį ir rakto ilgį, tada stulpeliai yra perstatomi (keičiama jų išdėstymo tvarka) pagal pradinį raktą, o galiausiai simboliai yra surašomi eilutėmis – taip gaunamas pradinis tekstas.

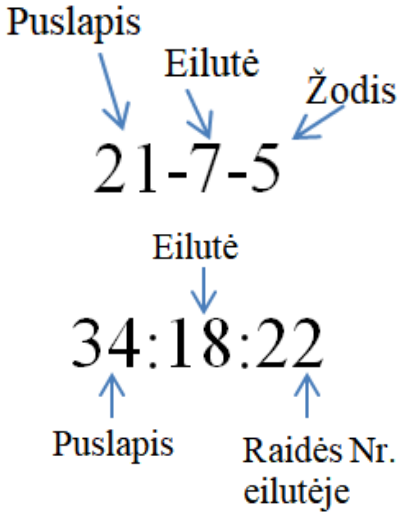
Užduotis

Kritiškai įvertinkite šio simetrinio šifravimo metodo saugaus duomenų perdavimo galimybę. Kaip galima būtų patobulinti šį metodą? Naudodami, pavyzdžiui, raktą „52143“ ar kitą užšifruokite trumpą patarlę. Pateikite ją draugui, siūlydami dešifruoti.

„Knyginis šifras“ *(angl. „Book cipher“)*

Šiame šifre knyga, koks nors kitas tekstas, ar specialiai sukurta kodų knyga naudojama kaip raktas, kurį turi abu komunikacijos dalyviai ir laiko jį paslaptyje. Jie naudoja puslapių, eilučių, žodžių ar raidžių eilutėje numerius žinutėms užšifruoti arba iššifruoti. Galima nustatyti taisykles, kurios padės gavėjui suprasti, kada naudoti žodžių metodą ir kada - raidžių metodą. Jei abu – ir siuntėjas, ir gavėjas – sutaria dėl šių taisyklių iš anksto, tai padės efektyviai keistis šifruota informacija.

Pavyzdžiui, jei nuspręsite, kad trys skaičiai, atskirti brūkšniais (pvz., 21-7-5), reiškia žodį, o skaičiai, atskirti dvitaškiais (pvz., 27:7:18), reiškia raidę, tai bus aišku gavėjui.



Knyginis šifras: žodžių ir raidžių kodavimo pavyzdžiai

Pavyzdys:
Tarkime, norite užšifruoti žinutę **„ALGIS IŠVYKO“**. „ALGIS“ galite užšifruoti naudojant raidžių metodą, o „IŠVYKO “ naudojant žodžių metodą.
„ALGIS“ naudojant konkrečia knygą gali būti užšifruotas kaip „27:7:18 33:5:1 15:8:2 2:3:3 1:2:9“ (tai reiškia, kad „A“ yra 27 puslapyje, 7 eilutėje, 18 pozicijoje, „L“ yra 33 puslapyje, 5 eilutėje, 1 pozicijoje) ir t.t.
Žodis „IŠVYKO“ gali būti užšifruotas kaip „25-5-5“ – 25-as puslapis, 5-a eilutė, 5-as žodis ir t. t.
Visa užšifruota žinutė bus: „27:7:18 33:5:1 15:8:2 2:3:3 1:2:9 25-5-5“.

Užduotis. Naudodami internete PDF formatu publikuojamą Vinco Mykolaičio Putino knygą „Altorių šešėly“ . http://antologija.lt/files/pdf/vincas-mykolaitis-putinas-altoriu-sesely.pdf (žr. 2023-09-20), iššifruokite žinutę: „13-10-11 117-5-14 8-9-1 84-5-1 84-5-2“. Pabandykite šiuo simetriniu metodu užšifruoti mokytojo pateiktą ar savo žinutę. Duokite klasės draugui ją iššifruoti. Diskutuodami nustatykite šio šifravimo metodo silpnąsias ir stipriąsias puses.

Šifravimo automatizavimo era. Kompiuterizavimo priešaušris

https://www.ourbow.com/take-a-daytrip-from-london-bletchley-park/

19-ojo amžiaus pabaigoje ir 20-ojo amžiaus pradžioje labai padaugėjo bandymų automatizuoti šifravimo procesus, kuriant vis sudėtingesnes sistemas.

Vienas ryškiausių pavyzdžių – **šifravimo mašina *Enigma***. *Enigma* turėjo klaviatūrą, o ruošiamas šifruotas tekstas automatiškai buvo šifruojamas vidinių mechanizmų. *Enigma* buvo šifravimo įrenginys, kurį Antrojo pasaulinio karo metais daugiausiai naudojo vokiečiai. Jis buvo naudojamas slaptiems pranešimams užšifruoti ir iššifruoti, todėl sąjungininkams buvo sunku perimti ryšį. Didžiojoje Britanijoje buvo svarbiausias šifro analizės centras, kuriame dirbo šimtai žmonių, tarp jų ir Alanas Tiuringas *(Alan Turing)* – vienas iš tų, kurie padėjo atskleisti *Enigma* paslaptį.

Užduotis

Nustatykite, kurios iš pateiktų simetrinių šifravimo metodų yra saugiausiais. Pagrįskite tai argumentais diskutuodami su bendraklasiais.

Šifravimo metodų gausa

https://www.wallpaperflare.com/dance-disco-dubstep-edm-electro-electronic-hip-hop-house-wallpaper-peprk

Yra labai daug svetainių, kur pateikiama įvairių šifravimo metodų bei šifravimo – dešifravimo įrankių, pavyzdžiui:

Boxentriq (**https://www.boxentriq.com/**)

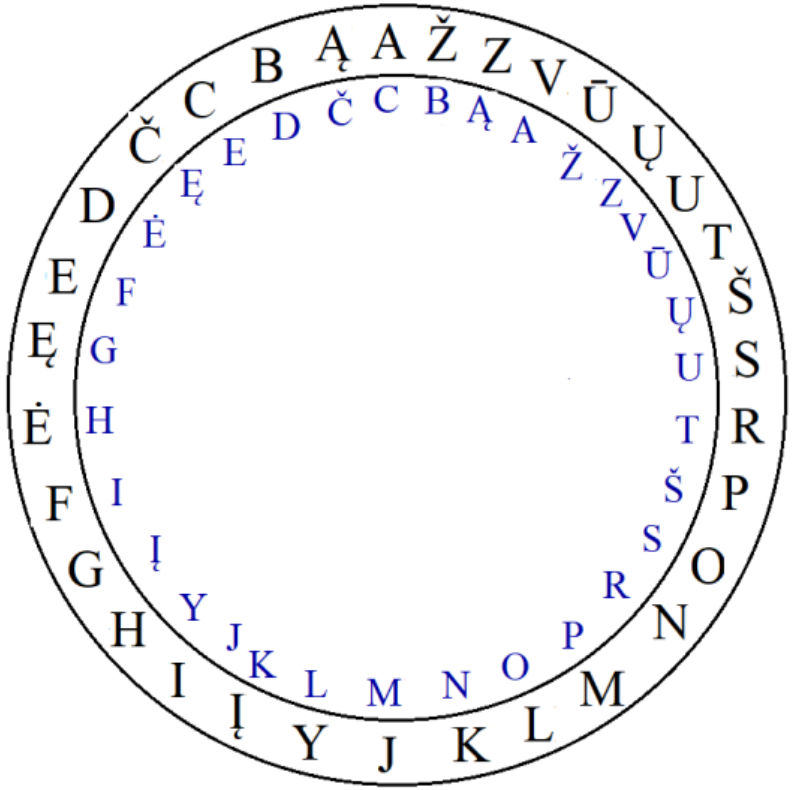
CacheSleuth (**https://www.cachesleuth.com/**)

dCode (**https://www.dcode.fr/**)


(Dancing men cipher)

Užduotis (tema 29.3.3.). Klasė suskirstoma į kelias grupes po, pavyzdžiui, 3–5 mokinius.
Scenarijus. Yra numatytas klasės vakarėlis, kuriame dalyvaus ir mokytojai. Kiekviena mokinių grupė ruošia staigmeną vienam pasirinktam vakarėlio dalyviui iš kitos grupės arba mokytojui. Dirbant grupėje ir naudojant vieną iš nagrinėtų ar šioje skaidrėje pateiktose nuorodose aprašytų metodų arba šifravimo įrankį, reikia užšifruoti numatytos vakarėlio staigmenos trumpą aprašymą. Baigus šifravimą, grupės pasikeičia užšifruotais pranešimais (raktą laiko paslaptyje). Nutariama, iki kada mokiniai bandys dešifruoti pranešimus (gali tai daryti ir namuose). Nustatytu laiku grupės atstovai visai klasei praneša apie nustatytus šifravimo metodus, juos apibūdina, paskelbia iššifruotą pranešimą, pasako, kas buvo sunkiausia, išrenka saugiausią panaudotą šifravimo metodą.

Užduotys



1 užduotis. Užšifruokite tekstą Cezario šifru naudodami poslinkius:

a) 2

b) 7

c) 20

NEPAPRAŠĘS LEIDIMO NESKELBK VIEŠAI KITŲ NUOTRAUKŲ

2 užduotis. Tekstas užšifruotas Cezario šifru, tačiau raidžių poslinkis nežinomas. Žinoma tik tai, kad originaliame tekste dažniausiai vartojama raidė A. Iššifruokite tekstą (tarp žodžių tarpų nepalikta)

BDŪDŲEDZTŪZTJDŽŪLŽUDRDŠJTOH

3 užduotis. Panaudodami Cezario šifro lentelę iškoduokite žodį ĄŽBYIĄĘG

4 užduotis. Kaip sudaryta Cezario šifro lentelė, jei užšifravus žodį MOKYKLA jis užrašomas taip: RŠOMOPČ

A	Ą	B	C	Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J	K	L	M	N	O	P	R	S	Š	T	U	Ų	Ū	V	Z	Ž
Č	D	E	Ę	Ė	F	G	H	I	Į	Y	J	K	L	M	N	O	P	R	S	Š	T	U	Ų	Ū	V	Z	Ž	A	Ą	B	C