moks.link/bhqh

Kaip šifruojame duomenis?

Prisiminsime saugų elektroninių laiškų, žinučių, pokalbių siuntimą.

Sužinosime, kas yra slaptasis raštas.

Išsiaiškinsime, kaip užšifruojami ir iššifruojami duomenys, informacija.

PRISIMENAME

Siunčiami elektroniniai laiškai, telefoninės žinutės užšifruojami taip, kad juos galėtų perskaityti tik siuntėjas ir gavėjas. Šifruoti galima įvairiai. Tikriausiai esate rašę slaptas žinutes, taikydami įvairias gudrybes, slėpdami tekstą, kad kiti jo neperskaitytų. Pagalvokite ir pateikite pavyzdžių.

SUŽINOME IR IŠSIAIŠKINAME

Prieš 5 400 metų žmonės sukūrė pirmąjį raštą. Kai vis daugiau žmonių išmoko suprasti rašto ženklus, atsirado poreikis įslaptinti kai kurią informaciją. Taip atsirado slaptasis raštas. Pirmieji bandymai naudotis slaptuoju raštu datuojami maždaug 3 500 metų prieš Kristų. Iš pradžių slaptajame rašte buvo taikomas raidžių keitimas vietomis. Atsirado kriptogrāfija – mokslas, tiriantis užšifravimo ir iššifravimo būdus. Viduramžiais šis mokslas tapo matematikos dalimi. Sukūrus kompiuterius ir internetą, duomenų saugumo klausimai tapo itin svarbūs. Nuo tada informatikai ėmė rūpintis saugių slaptųjų raštų kūrimu. Į slaptąją kalbą išverstas tekstas vadinamas **užšifrúotu tekstù**, o jo vertimas atgal į originalų tekstą – **iššifrāvimu**.

Kaip parašyti slaptą žinutę?

Aras ir Mantė naudoja du slaptuosius raštus, kad galėtų keistis tik jiems suprantamomis žinutėmis. Jei kas ir pamato šias žinutes, jų nesupranta. Pirmąjį slaptąjį raštą Aras naudoja rašydamas žinutes Mantei, o antrąjį – Mantė rašydama Arui. Užšifruodami žinutes, Mantė ir Aras keičia teksto raidžių eiliškumą. Joris smalsus ir norėtų sužinoti, ką Aras rašo Mantei. Jam pavyksta perimti du Aro ir Mantės laiškus:

TAIKOME

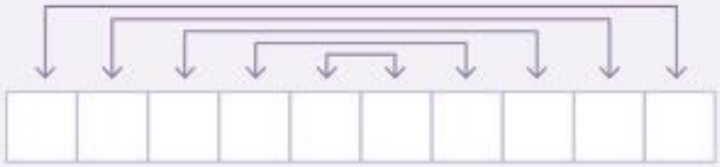
Padėkite Joriui perskaityti abi žinutes. Pastebėta, kad Aro rašyta žinutė prasideda ARGALĖTUME

Aro užšifruotas žodis ALGORITMAS atrodo taip:

Aras šifruoja keisdamas raides vietomis: pirmąją ir antrąją, trečiąją ir ketvirtąją, penktąją ir šeštąją ir t. t. Tokį šifravimą galima pavaizduoti schema:

Originalus tekstas	A	L	G	O	R	I	T	M	A	S
Užšifruotas tekstas	L	A	O	G	I	R	M	T	S	A

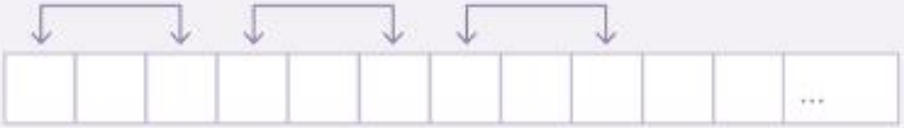
Mantė šifruoja kitaip keisdama raides: pirmąją – su paskutine, antrąją – su priešpaskutine ir t. t. pagal štai tokią schemą:



Mantės užšifruotas tas pats žodis ALGORITMAS užrašomas SAMTIROGLA.

1. Užšifruokite Aro būdu savo vardą ir pavardę.

2. Tomas savo šifravimo būdą pavaizdavo tokia schema:



Iššifruokite šį tekstą naudodamiesi Tomo šifravimo metodu:

UASKOGVASLSOTPAOŽAIŽDPSUITAMIKESOEIVSOTE

Tai įdomu

Elektromechaninė šifravimo mašina „Enigma" (išvertus iš graikų kalbos – mįslė) yra vienas įdomiausių išradimų, naudotų Antrajame pasauliniame kare. Mašina kasdien keitė šifrą, todėl karinės žinutės buvo šifruojamos vis kitu būdu. Vadinasi, iššifravus vieną žinutę, nereikšdavo, kad pavyks iššifruoti ir kitą. Vis dėlto britų matematikas ir informatikas Alanas Turingas (*Alan Turing*) sugalvojo, kaip „nulaužti" „Enigmos" šifrą.

11 pav. Elektromechaninė šifravimo mašina „Enigma"

Kaip naudoti Cezario šifrą kitaip?

Cezario šifras gali būti vaizduojamas ratais, kai išoriniame apskritime yra naudojamos pranešimo raidės, o šifruotas pranešimas rašomas keičiant raides tokiomis raidėmis, kurios per tris pozicijas yra nutolusios nuo išorinio apskritimo raidžių. Vidiniame rate tos raidės jau yra pasuktos. Jei tokie ratai yra pagaminti ir vidinis ratas gali sukiotis, tai nebūtina naudoti šifro raktą, lygų 3 raidėms. Galima naudoti ir kitus raidžių poslinkius arba net kelis skirtingus poslinkius.

12 pav. XVI a. knygos formos prancūziškas šifravimo aparatas

Kaip užšifruoti ir iššifruoti informaciją naudojant lenteles?

Kuriant slaptuosius raštus buvo naudojamos ir lengvai įsimenamos lentelės. Šis metodas buvo žinomas prieš 2 300 metų prieš Kristų Graikijoje ir Palestinoje.

Surašome visas abėcėlės raides iš eilės į lentelę (galime pasirinkti norimo dydžio lentelę):

	1	2	3	4	5	6	7	8
■	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

Lentelės eilutes pažymime sugalvotais simboliais, pavyzdžiui: ■, ◆, ▲ ir ●. Stulpelius sunumeruojame. Kad perskaitytumėme užšifruotą tekstą, svarbu tik įsiminti lentelės dydį (eilučių ir stulpelių skaičių) ir papildomus simbolius. Kiekviena raidė užšifruojama eilutės ir stulpelio, kuriuose yra ta raidė, simbolių kombinacija. Štai taip atrodytų užšifruota abėcėlė:

■1	■2	■3	■4	■5	■6	■7	■8
◆1	◆2	◆3	◆4	◆5	◆6	◆7	◆8
▲1	▲2	▲3	▲4	▲5	▲6	▲7	▲8
●1	●2	●3	●4	●5	●6	●7	●8

Kaip atrodo „geležinkelio tvorelės“ šifras?

Šiuo atveju pranešimo žodžiai užrašomi įstrižai. Pasirenkamas įstrižainės ilgis, nusibraižomas tinklelis. Žodžiai atskiriami tarpais. Užšifruokime, pavyzdžiui, tokį sakinį: LIETUVOS SOSTINĖ VILNIUS

L		E		U		O				O		T		N				I		N		U	
	I		T		V		S		S		S		I		Ė		V		L		I		S

Užšifruotas tekstas: LEUO OTN INUITVSSSIĖVLIS

Tą patį tekstą užšifruokime, kai įstrižainės ilgis lygus 3.

L				U							T							N				
	I		T		V		S		S		S		I		Ė		V		L		I		S
		E				O				O				N				I				U	

Užšifruotas tekstas: LU T NITVSSSIĖVLISEOONIU

Tą patį tekstą užšifruokime, kai įstrižainės ilgis lygus 4.

L						O					T						I						
	I				V		S				S		I				V		L				S
		E		U					O				N						N		U		
			T					S						Ė						I			

Užšifruotas tekstas: LOTIIVSSIVLSEU ON NUTSĖI

Šis šifras dar vadinamas zigzago šifru. Kaip manote, kodėl?

Tai įdomu

Kriptologijos mokslui priskiriamas menas iššifruoti tekstus, net jei nežinoma, kokiu būdu jie buvo užšifruoti. Jei kažkam pavyksta perprasti užšifruotą tekstą, kurio šifras nežinomas, sakoma, kad „pavyko nulaužti šifrą". Šifrų atkūrimas vadinamas kriptoanalize. Vienas jos metodų yra dažnumų analizė. Atliekant dažnumų analizę, remiamasi faktu, kad įvairių kalbų abėcėlės raidės vartojamos nevienodai dažnai. Pavyzdžiui, lietuvių kalboje dažniausia raidė yra I: tekste, kurį sudaro 100 raidžių, ji sutinkama maždaug 14 kartų. Antroji pagal dažnumą raidė yra A (maždaug kas vienuolikta raidė). Todėl reikėtų suskaičiuoti užkoduoto teksto simbolius ir daryti prielaidą, kad dažniausias užšifruoto teksto simbolis yra raidė I, o antras pagal dažnumą – raidė A.

ĮTVIRTINAME IR ĮSIVERTINAME

1. Aras, kaip pamenate, šifruoja keisdamas dvi greta esančias raides vietomis. Jo užšifruota žinutė:
ONĖRIČUAUTĖRITOROBĄTAPOMOKSMURŠOIT
Iššifruokite ją.

2. Užšifruokite tekstą Cezario šifru naudodami poslinkius: a) 3; b) 7; c) 20.
NEPAPRAŠĘS LEIDIMO NESKELBK VIEŠAI KITŲ NUOTRAUKŲ

3. 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

4. Naudodami „geležinkelio tvorelės" šifrą ir žinodami, kad įstrižainė lygi 3, iššifruokite tekstą:
TĄA I AJIR RUĄPŽNINLIĖEKDGASEM
Tai sunkoka užduotis. Kad būtų lengviau spręsti, pateikiame tinklelį ir pirmąją eilutę:

T			Ą			A						I						A			J	

5. Tarkime, gavote štai tokią užšifruotą žinutę:
USTŽĘJMTNAUBĮČTVGTNČTĘETVECTČVZĮČPČMCĮĘSĘČ
Žinote, kad naudotas Cezario šifras ir kad raidė Š buvo pakeista raide B, o T – raide C. Ar pavyks perskaityti užšifruotą žinutę?

6. Remdamiesi aprašytos šifravimo lentelės pavyzdžiu, užšifruokite šį tekstą:
DUOMENŲSAUGUMASBUVOSVARBUSNETSENOVĖSLAIKAIS

7. Panagrinėkime įdomesnį interaktyvų šifrą (taikoma anglų kalbos abėcėlei). Atvėrę nuorodą galime sukti vidinį (pele sukamas mėlynas skrituliukas) ar išorinį ratą (pele sukamas raudonas žiedas). Pasirinkus norimą raidžių keitimą, galima užšifruoti įvairias frazes. Užšifruokite žodį LIETUVA.

Sukurkime

8. **Sugalvokite** savo slaptąjį raštą, kuris būtų paremtas raidžių sukeitimu.
a) **Pavaizduokite** savo šifravimo būdą schema.
b) Naudodamiesi savo sugalvotu būdu, **užšifruokite** ilgą žodį ar sakinį. **Pasiūlykite** savo draugams šį užšifruotą tekstą iššifruoti ir **pridėkite** šifravimo schemą.

KO IŠMOKAU? KAIP MAN SEKĖSI?