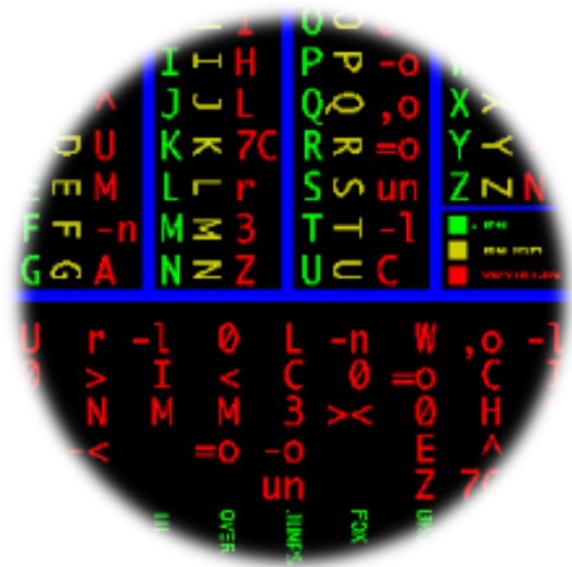


Šifravimas



Šifravimas

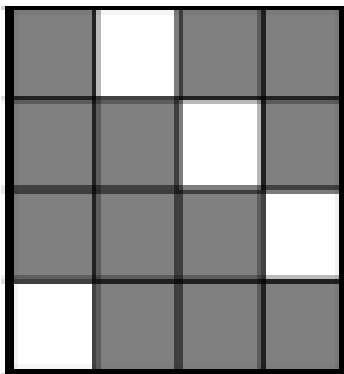
Žmonėms nuolat kyla poreikis apsaugoti svarbią informaciją: karo metu, kuriant naujas technologijas, produktus, meno kūrinius, saugant asmens tapatybę, saugant valstybines paslaptis ir daugybe kitų atvejų.

Apibrėžimai

- **Šifravimas** – tai informacijos kodavimas su tikslu tą informaciją įslaptinti. Šifravimas susijęs su informacijos užšifravimu ir iššifravimu
- **Užšifravimas** – tai specialus informacijos kodavimo būdas siekiant ją įslaptinti (paslepiama informacijos prasmė)
- **Iššifravimas** – tai procesas, kurio metu grąžinama pradinė užšifruotų duomenų forma.
- Užšifruota informacija gali būti iššifruojama tik žinant raktą. Raktas – tai priemonė užšifruotiems duomenims iššifruoti.

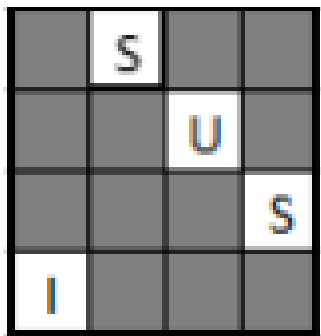
Kvadratų šifras

- Norime saugiai perduoti pranešimą „SUSITINKAME RYTOJ“. Šis pranešimas sudarytas iš 16 raidžių.
- Pranešimo užšifravimui pasirenkame 16 langelių kvadratą ir jame iškerpame 4 langelius.
- Žinoma, langeliai iškerpami specialiu būdu, kuris tuoju paaiškės. Tarkime, kad pasirinkome tokį būdą:



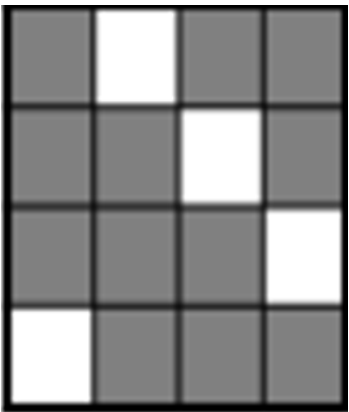
Kvadratų šifras

- Specialiai parengtas 16 langelių kvadratas, kurio 4 balti langeliai yra kiauri.
- Nubraižome lygiai tokį patį 16 langelių kvadratą. Ant jo uždedame parengtąjį ir parašome į kiaurus langelius nuo viršaus iš kairės į dešinę 4 pirmąsias pranešimo raides:
- Tada uždėtąjį kvadratą pasukame 90 laipsnių kampu prieš laikrodžio rodyklę.



Kvadratų šifras

- ir vėl uždėję užrašome kitas keturias raides.
- Viršutinį kvadratą pasukus



Kvadratų šifras

- Dar kartą prieš laikrodžio rodyklę, tekstas bus toks:

	S	T	A
M	I	U	
N	E		S
I		R	K

. Po trečio posūkio

Y	S	T	A
M	I	U	T
N	E	O	S
I	J	R	K

Kvadratų šifras

- Bus užšifruotas visas pranešimas:
- Siunčiamas toks pranešimo tekstas „YSTAMIUTNEOSIJRK“.
- Gavėjas privalo turėti identišką kvadratą, kad galėtų iššifruoti tekstą.
- Jei pranešimas yra ilgesnis, galima naudoti ir didesnį kvadratą.
Kiekviename $4n^2$ langelių kvadrato galima išpjauti n^2 langelių, kad tris kartus pasukus 90 laipsnių kampu prieš laikrodžio rodyklę (arba kaip yra sutarta) galima būtų įrašyti pranešimą į visus mažus $4n^2$ langelius.

Cezario šifras

- Cezario šifras yra gerai žinoma kriptosistema, kurią naudojant raidės pasislenka per kelias pozicijas abėcėlėje.
- Per kiek perstumti raides nustato šifro raktas. Tradiciškai su Cezario šifru siejamas kiekvienos raidės pakeitimas nutolusia nuo jos abėcėlėje trečiaja raide, einant per abėcėlę apskritimu.
- **Pavyzdžiui, jei naudojama lietuviška abėcėlė**
- **A AĄ B CČ D E Ė F G H I Į J K L M N O P R S Š T U Ū V Z Ž** ir raktas yra 3, raidė A tampa C, Aą tampa Č ir t. t., o raidė Ž tampa B.
- Žodis „ŠIFRAS“ užšifruojamas kaip „ŪJITCU“.

Cezario šifras

- Dažnai Cezario šriftas vaizduojamas koncentriniais raidžių ratais, šifruotas pranešimas rašomas keičiant raides tokiomis raidėmis, kurios per tris pozicijas yra nutolusios.
- Vidiniame rate tos raidės jau yra pasuktos. Jei tokie ratai yra pagaminti ir vidinis ratas gali sukrotis, tai nebūtina naudoti šifro raktą lygų trimis raidėms. Galima naudoti ir kitus raidžių poslinkius arba net kelis poslinkius.



Viženero šifras

- Viženero šifrui (pranc. Chiffre de Vigenère) raktu naudojame pasirinktą žodį.
- Tarkime, kad raktas yra žodis KODAS ir norime užšifruoti žodį (pranešimą) AUTOSTEREOGRAMA (autostereograma – kompiuterio sukurtas paveikslas, kuris iš pirmo žvilgsnio atrodo abstraktaus dizaino, tačiau įsižiūrėjus jame išryškėja erdvinės figūros)

K	O	D	A	S	K	O	D	A	S	K	O	D	A	S
A	U	T	O	S	T	E	R	E	O	G	R	A	M	A

Viženero šifras

- Kiekvieną rakto raidę naudojame kaip Cezario šifro poslinkį ir užšifruojame kiekvieną pranešimo raidę. Norėdami užšifruoti raidę A užšifruojame rakto raide K (poslinkis 16) ir gauname K ($0 + 16$).
- Tada toliau U raidei imama kodo O raidė, ji yra 20, todėl $(26 + 20) \bmod 32 = 14$ ir bus Y raidė.

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
0	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

Viženero šifras

Gaunamas kodas: K Y Z O Y F U Ū E H U G D M S.

K	O	D	A	S	K	O	D	A	S	K	O	D	A	S
A	U	T	O	S	T	E	R	E	O	G	R	A	M	A
K	Y	Z	O	Y	F	U	Ū	E	H	U	G	D	M	S

Užšifravimui ir iššifravimui naudojamos abėcėlės lentelės, vadinamos *tabula recta* arba Viženero kvadratais (lentelėmis). Lietuviškos abėcėlės Viženero lentelę sudaro eilutės po 32 simbolius, o kiekviena eilutė pasislenka keliomis pozicijomis. Lentelėje pateikiami 32 skirtingi Cezario šifrai.

Geležinkelio tvorelės šifras

Panagrinėkime du geležinkelio tvorelės (angl. *rail fence*) atvejus.

1. Pranešimą „**VAIKAI ATVYKSTA RYTOJ**“ užrašykime 4 raidžių aukščio lauzte, primenančia geležinkelio tvorelę, skirtą apsaugoti bėgius nuo užpustymo.

V				A				T			J
	A				I		T			S	
		I		A				V		K	
			K						Y		

Skaitydami užšifruotą pranešimą eilutėmis, gauname „**VATJAITS AOIAVKRTKY**“.
Toku atveju šifro raktas yra 4.

2. Dabar tą patį pranešimą parašykime stulpeliais po du simbolius:

V		I		A		A		V		K		T		R		T		J
	A		K		I		T		Y		S		A		Y		O	

Skaitydami pranešimą eilutėmis, gauname „**VIAAVKTRTJAKITYSAYO**“.

Teksto šifravimo RSA šifru pavyzdys

Lietuviškos abėcėlės raides pavaizduokime skaičiais, o tarpą skaičiumi 32:

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Užduotis

1 UŽDUOTIS

Agnė ir Berta turi slaptą kalbą. Kiekvieną raidę žodyje jos pakeičia raide einančia po jos. Savo kalbai jos naudoja anglų kalbos abėcėlę ir žodžius, kuriuos užšifruoja (pavyzdžiui a yra keičiama raide b, b su c ir t.t., z yra keičiama raide a). Kokią žinutę Agnė siunčia Bertai: **IFMMP CFSUB ?**

Atsakymas:

UŽDUOTIS

- Adomas ir Jonas turi slaptą kalbą. Kiekvieną raidę žodyje jie pakeičia raide einančia po jos. Savo kalbai jie naudoja anglų kalbos abėcėlę ir žodžius, kuriuos užšifruoja (pavyzdžiui a yra keičiama raide b, b su c ir t.t., z yra keičiama raide a). Padėk Adomui užšifruoti savo žinutę: **NICE COMPUTER**

Atsakymas: **OJDF DPNQVUFS**

3 UŽDUOTIS

Erika su draugais rašo žinutes slapta kalba, kiekvieną raidę jie pakeičia skaičiumi iš dviejų ženklų, pradedant nuo 00, taigi A yra 00, B yra 01, C yra 02 ir t.t. (naudojamos anglų abėcėlės raidės) Kokią žinutę Erika parašė savo draugams?

06 14 14 03 12 14 17 13 08 13 06

Atsakymas: Good morning

4 UŽDUOTIS

Benas nori pasidalinti slapta žinute su savo draugais, kiekvieną raidę jis pakeičia skaičiumi iš dviejų ženklų, pradedant nuo 00, taigi A yra 00, B yra 01, C yra 02 ir t.t. (naudojamos anglų abėcėlės raidės). Kaip užsišifruos ši žinutė:

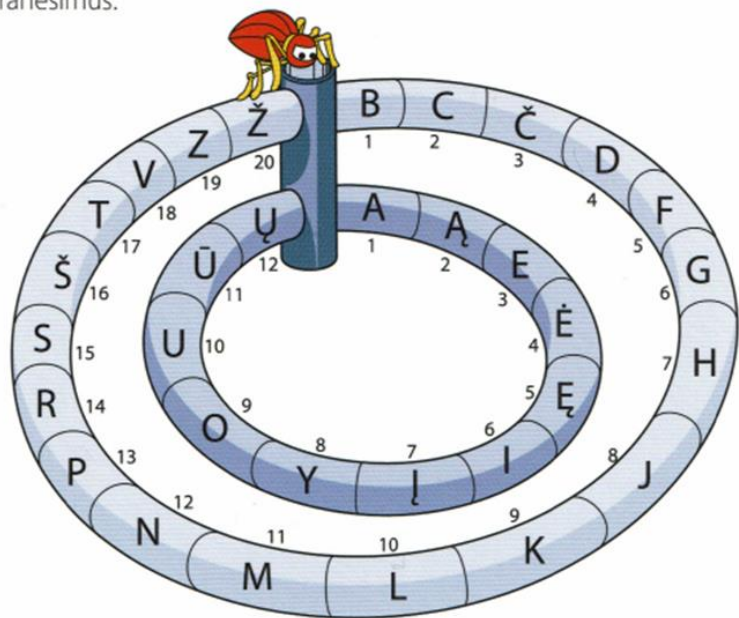
INTERESTING GAME

Atsakymas: 08 13 19 04 17 04 18 19 08 13 06 06 00 12 04



VORAS VAMZDYJE

Bebras sukonstravo vorą robotą. Voras ropoja vamzdžiais pagal laikrodžio rodyklę, kai reikia, iš didžiojo vamzdžio perbėga į mažąjį jungiamuoju vamzdeliu. Ropodamas ir liesdamas raides užkoduoja pranešimus.



Perskaitykite šį voro užkoduotą pranešimą:

11_D 10_M 11_D 15_D 13_D 1_M 17_D 6_M 12_D 9_D 1_M 20_D 11_D 9_M 6_D 10_M 15_D

18_D 9_M 14_D 1_M 15_D