Informacijos 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.

Kodavimas

Kodavimas - tai **vienos abėcėlės ženklų keitimas kitos abėcėlės ženklais**.

- Kodavimas reikalingas tam, kad pranešimas būtų perduodamas *kuo tiksliau*, kad jis būtų kuo *mažiau iškraipomas*, kad jį suprastų gavėjas ir kad būtų galima persiųsti pasirinktu mainų kanalu, neturint tikslo jų užslaptinti.

Kodavimas – tai :

- informacijos apdorojimas, laikymas naudojant *sutartinių ženklų sistemą*;
- atskiro objekto ar jo savybės žymėjimas skaičiumi arba *tam tikros abėcėlės ženklais*;
- programos *užrašymas kompiuterine kalba*, naudojant sutartų ženklų sistemą.

Šifravimas

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.

Nors ir kodavimas, ir šifravimas yra metodai, kurie *transformuoja duomenis į skirtingus formatus*, ***tikslai***, kurių jais siekiama, yra ***skirtingi***.

- **Kodavimas** *atliekamas siekiant padidinti duomenų tinkamumą* naudoti skirtingose sistemose ir sumažinti saugojimui reikalingą vietą;

- **Kodavimas** atliekamas *naudojant viešai prieinamus metodus* ir jį galima lengvai pakeisti.

- **Šifravimas** *atliekamas siekiant išlaikyti duomenų paslaptį* nuo trečiųjų šalių.

- **Užšifruotų** duomenų *negalima lengvai iššifruoti*. Tam *reikia turėti specialią informaciją*, vadinamą raktu.

Šifravimas **naudojamas įvairiose srityse**, įskaitant chemiją, matematiką ir kompiuterių mokslą.

- *Chemijoje* šifravimas naudojamas siekiant *apsaugoti tyrimų duomenų konfidencialumą.*
- *Matematikoje* šifravimas naudojamas *ryšiams apsaugoti* ir jautriai informacijai apsaugoti.
- *Informatikos* moksle šifravimas naudojamas ***duomenims, perduodamiems internetu ir saugomiems kompiuterinėse sistemose, apsaugoti.***

Kriptologija

Su šifravimu susijęs ir nuo praeito amžiaus labai sparčiai besivystantis mokslas vadinamas **kriptologija**.

Kriptologija susideda *iš kriptografijos ir kriptoanalizės*.

Kriptografija – tai mokslas, nagrinėjantis informacijos *užšifravimo ir iššifravimo metodus*.

Kriptoanalizė – mokslas apie tai, kaip *įveikti užšifruotus tekstus*.

Žodis *kriptografija* kilo iš dviejų graikiškų žodžių, reiškiančių „slaptas raštas“.

Pagrindinis kriptografijos elementas yra kriptografinė sistema (kriptosistema) arba šifras.

Šiuolaikinė kriptografija – tai mokslo šaka, sprendžianti elektroninės informacijos saugos problemas.

Kadangi kasmet vis daugiau informacijos siunčiama skaitmeninėmis ryšio priemonėmis, labai svarbu užtikrinti jos saugumą, nes skaitmeninė informacija dažniausiai perduodama nesaugiais kanalais, pavyzdžiui, interneto ryšiu, ir gali būti pasiekiama beveik visiems

Klasikinės kriptosistemos

Klasikinės kriptosistemos (dar vadinamos *slaptojo rakto*, arba *simetrinėmis*) yra tos, kurios naudoja tą patį raktą šifravimui ir dešifravimui.

Yra du pagrindiniai klasikinių kriptosistemų tipai: *perstatų* šifras ir *keitinių* šifras.

- **Perstatų šifrai** (*Transposition*):
  - sukeičia vietomis raides pagal kokią nors taisyklę,
  - lieka tos pačios raidės, tik išdėstytos kita eilės tvarka.
- **Keitinių šifrai** (*Substitution*):
  - pakeičia kiekvieną raidę kita raide,
  - išlaiko raidžių eilės tvarką, bet pakeičia jų tapatybę.

Perstatų šriftai (1)

Skytalė - pirmasis istorijoje žinomas šifravimo įrenginys, kartu ir šifras. Naudotas Spartoje antikos laikais.

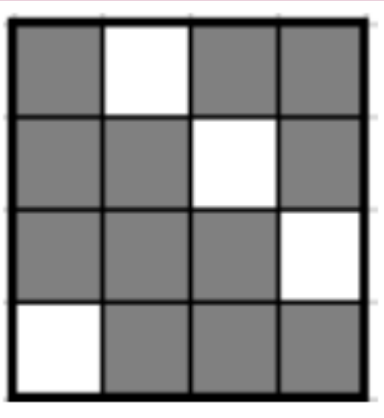
Ant tokios juostelės tekstą rašydavo taip:

- Užvyniodavo juostelę ant lazdelės taip, kad sluoksniai būtų šalia vienas kito, ir rašydavo ant jos eilutę po eilutės vis pasukant lazdelę.
- Užrašius tekstą, juostelę nuvyniodavo.
- Ant jos matosi tik pabiros raidės, kurios atrodo, kad yra išdėstytos be jokios tvarkos.
- Skaitant raides iš eilės užrašyto teksto perskaityti neįmanoma.
- Norint jį suprasti, juostelę reikia užvynioti ant tokio pat skersmens lazdelės.
- Taip užšifruoto teksto siuntėjas ir gavėjas turi turėti tokias pat lazdeles.

Kvadratų šifras

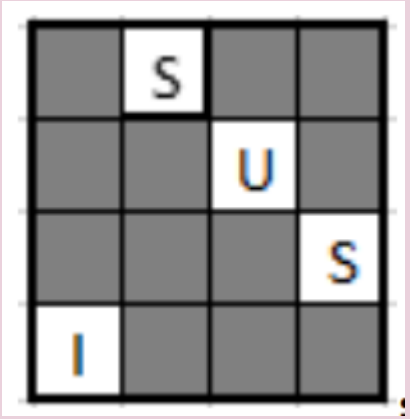
Norime saugiai perduoti pranešimą „SUSITINKAME RYTOJ“.

- Šis pranešimas sudarytas iš 16 raidžių
- Pranešimo užšifravimui pasirenkame 16 langelių kvadratą ir jame iškerpame 4 langelius.
- Žinoma, langeliai iškerpami specialiu būdu, kuris tuojau paaiškės



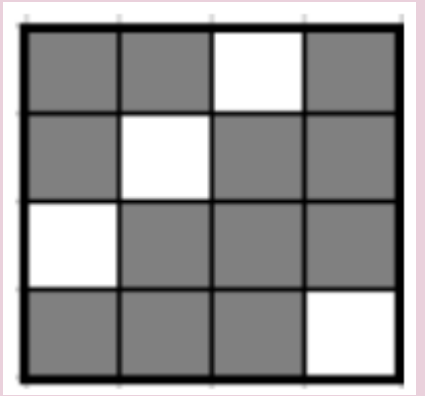
Kvadratų šifras (2)

- Sąsiuvinyje 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



Kvadratų šifras (3)

- uždėtąjį kvadratą pasukame 90 laipsnių kampu prieš laikrodžio rodyklę
- vėl uždėję užrašome kitas keturias raides
- Vėl pasukite kvadratą ir įrašykite sekančias 4 raides



- po trečio posūkio bus užšifruotas visas pranešimas:

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

pranešimo tekstas „YSTAMIUTNEOSIJRK“.

Kvadratų šifras (4)

Užduotis

Sugalvokite kelis pranešimą, kuris nebūtų ilgesnis nei 16 simbolių.

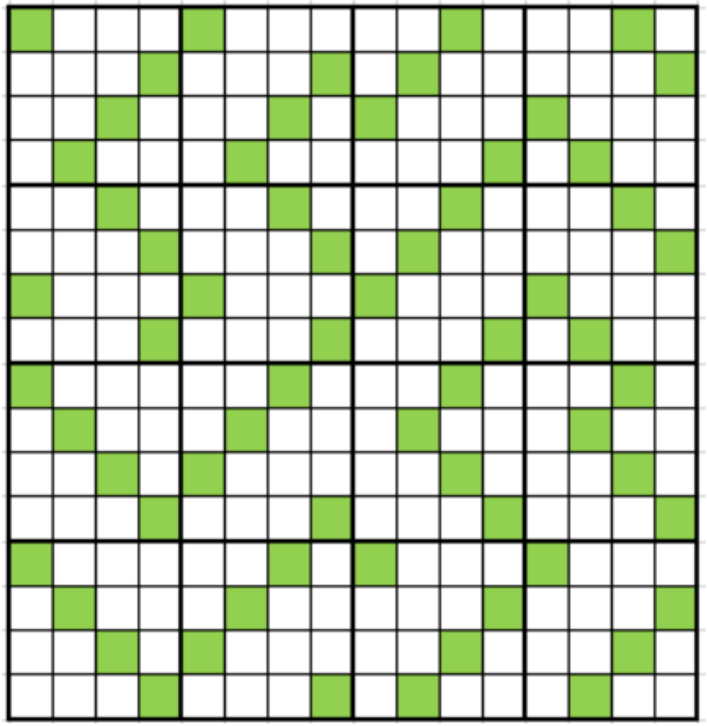
Užšifruokite jį

Kvadratų šifras (5)

Jei pranešimas yra ilgesnis, reikia naudoti ir didesnį kvadratą.

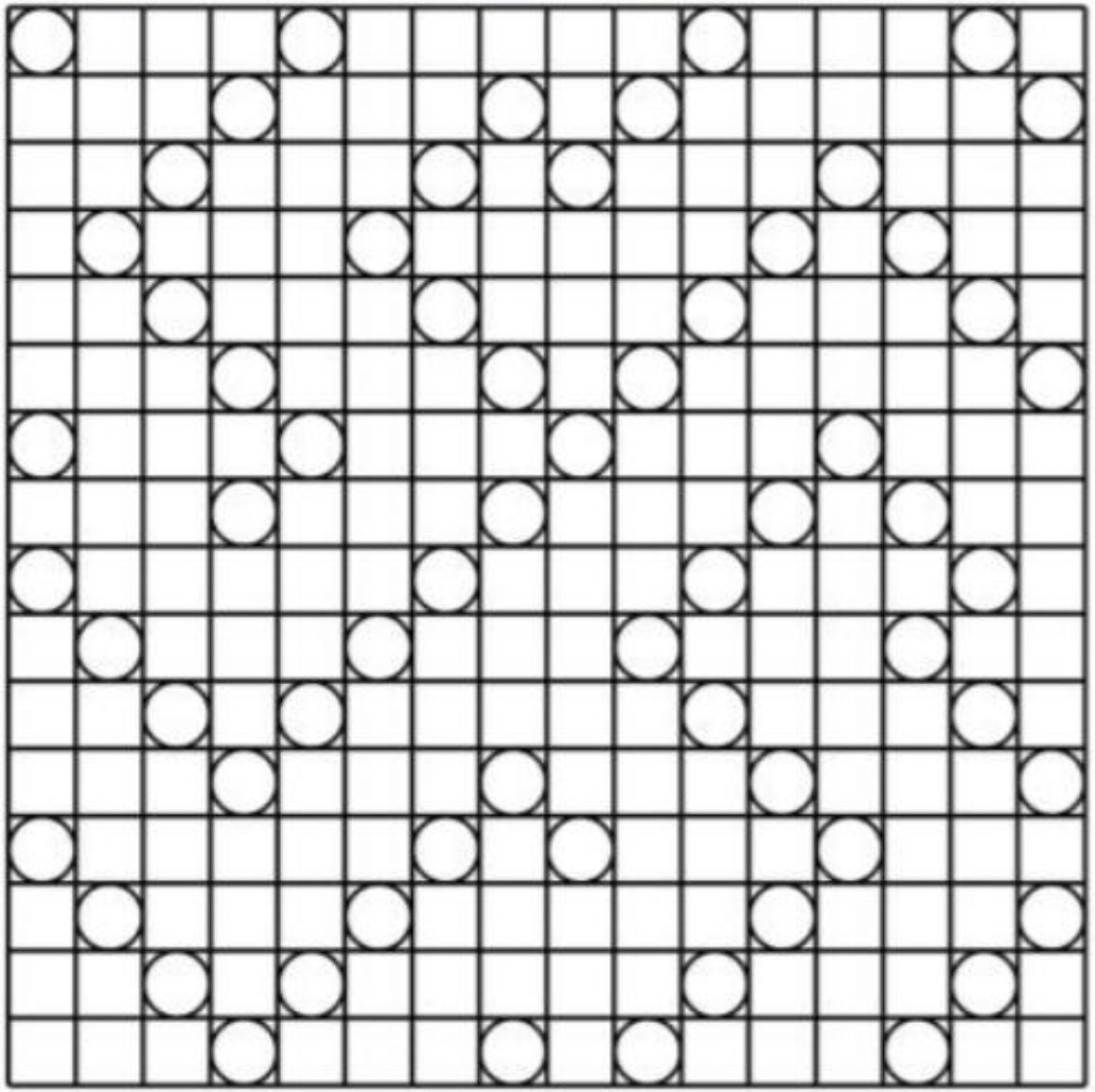
- Kiekviename $4n^2$ langelių kvadrate galima išpjauti n^2 langelių, kad tris kartus pasukus 90 laipsnių kampu prieš laikrodžio rodyklę (arba kaip yra sutarta) galima būtų įrašyti pranešimą į visus mažus $4n^2$ langelius

- Paveiksle pavaizduotas $4 \times 82 = 256$ langelių kvadratas, jame žalia spalva pažymėti 64 langeliai, kurie turi būti kiauri. Tokį kvadratą su sutarta posūkio taisykle turi pranešimo siuntėjas ir gavėjas.



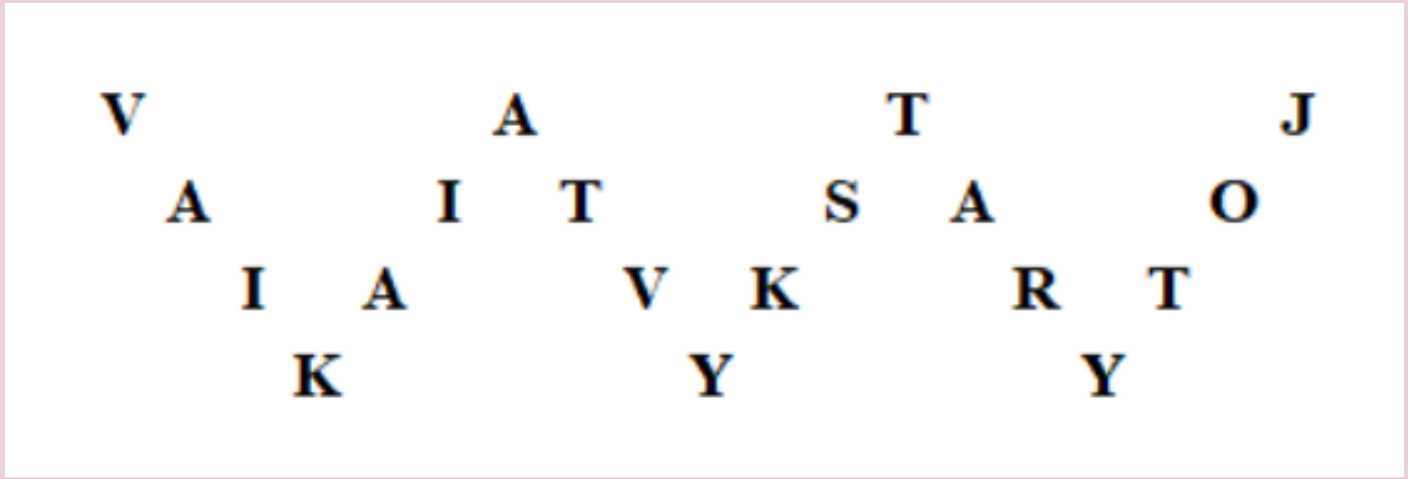
Fleissnerio kvadratų šifras

XVIII amžiuje naudoto Fleissnerio kvadratų šifro šablonas [Sta07]



Geležinkelio tvorelės šifras (1)

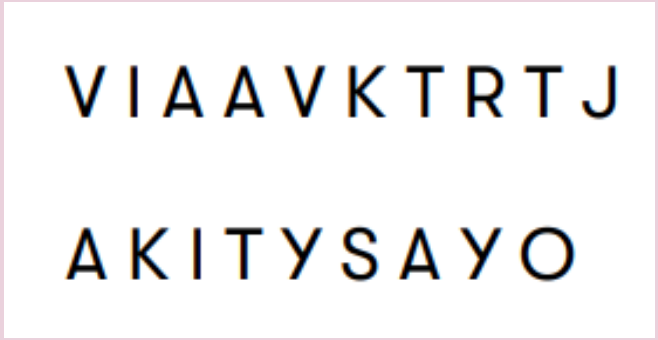
Pranešimą „VAIKAI ATVYKSTA RYTOJ“ užrašykime 4 raidžių aukščio laužte, primenančia geležinkelio tvorelę, skirtą apsaugoti bėgius nuo užpustymo.



- Skaitydami užšifruotą pranešimą eilutėmis, gauname „VATJAITSAOIAVKRTKYY“.
- Tokiu atveju šifro raktas yra 4.

Geležinkelio tvorelės šifras (2)

Dabar tą patį pranešimą parašykime stulpeliais po du simbolius:

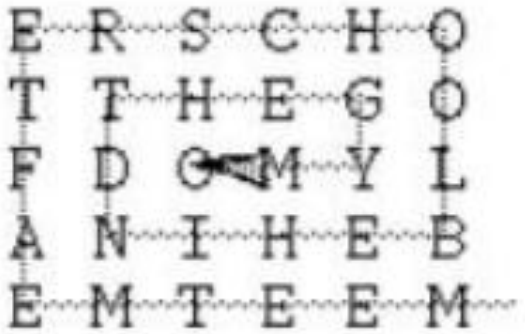


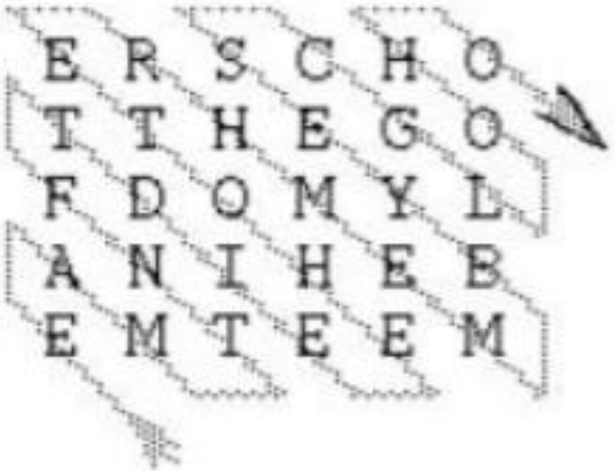
Skaitydami pranešimą eilutėmis, gauname „VIAAVKTRTJAKITYSAYO“.

Užduotis

Pasinaudodami geležinkelio tvorelės šifru ir keliais jo raktais užšifruokite jums patinkantį trumpą aforizmą.

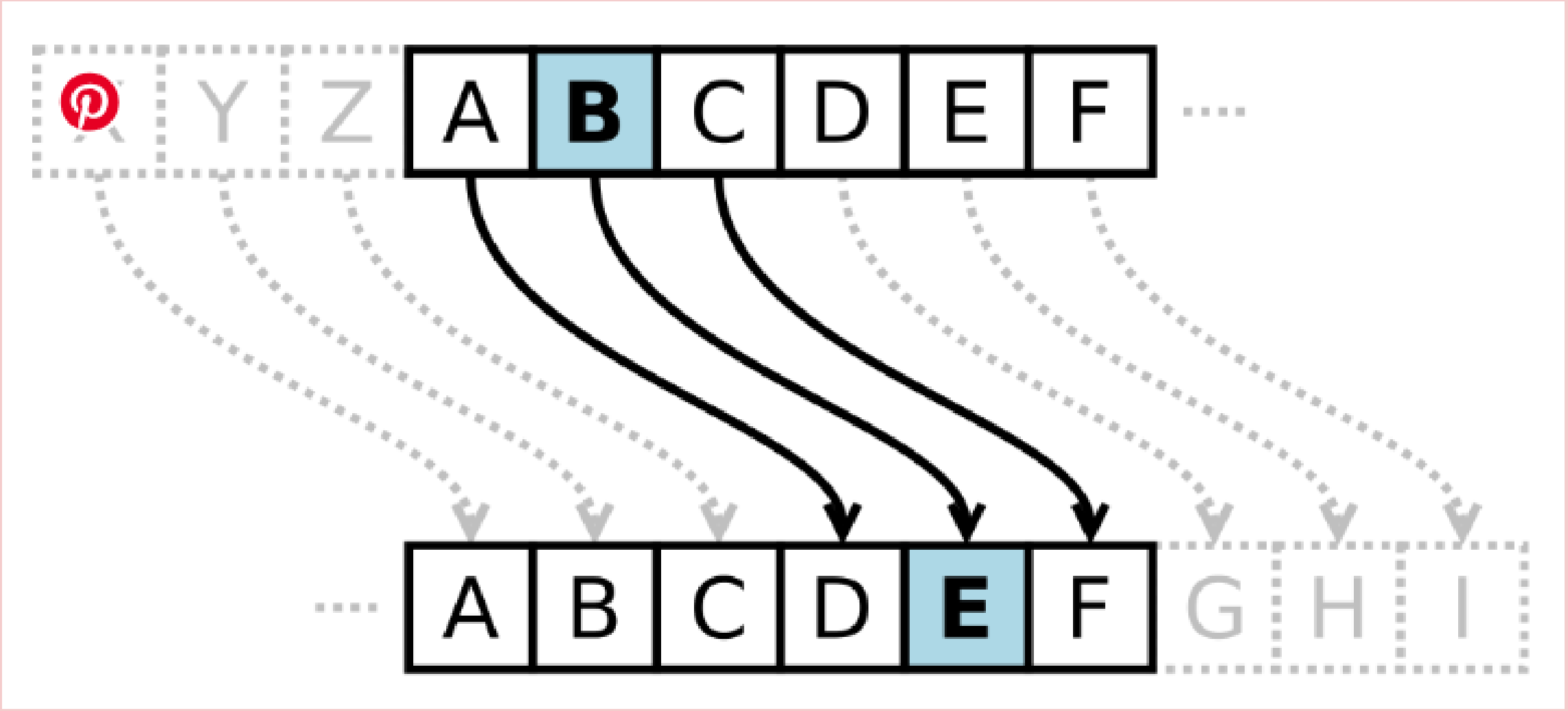
Perstatų šifrų pavyzdžiai (4): Kiti būdai





Keitinių šifrai: Cezario šifras (*Caesar Cipher*)

- Tai seniausias žinomas keitinių šifras.
- Pirmas patvirtintas šifro naudojimas kariniams tikslams.
- Naudotas Romos karvedžio Julijaus Cezario.
- Pakeičia kiekvieną raidę raide, stovinčia abėcėlėje trimis pozicijomis toliau:
- `a b c d e f g h i j k l m n o p q r s t u v w x y z`
- `D E F G H I J K L M N O P Q R S T U V W X Y Z A B C`
- Pavyzdys:
  - `susitikime po paskaitos`
  - `VXVLWLNLPH SR SDVNDLWRV`


X
Y
Z
A
B
C
D
E
F
A
B
C
D
E
F
G
H
I

Cezario šifras

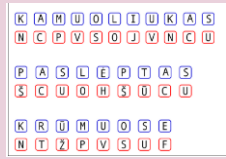
- *Užduotys*

1. Naudodami Cezario šriftą užšifruokite: ***KAMUOLIUKAS PASLĖPTAS KRŪMUOSE***

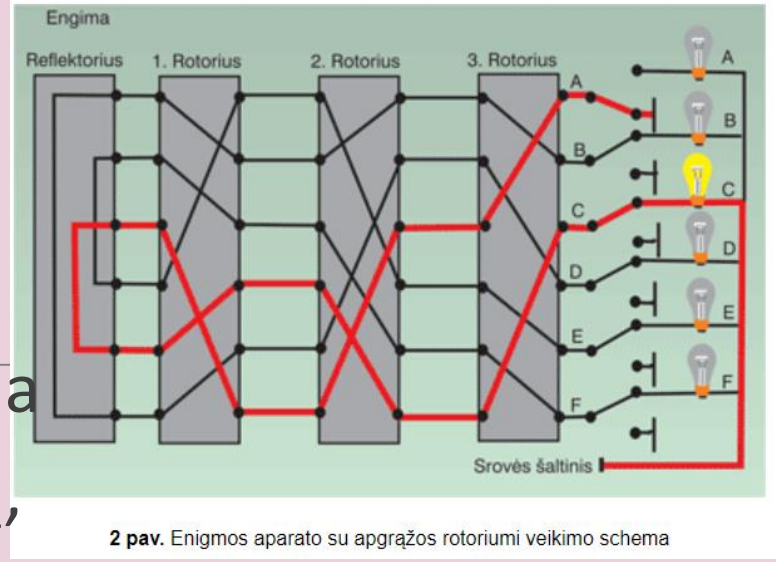
2. Parinkite aforizmų ir juos užšifruokite naudodami įvairias Cezario raktų vertes.

3. Išsiaiškinkite, kodėl šis šifras pavadintas Gajaus Julijaus Cezario (100–44 pr. m. e) vardu.

4. Išbandykite čia



Enigmos šifras

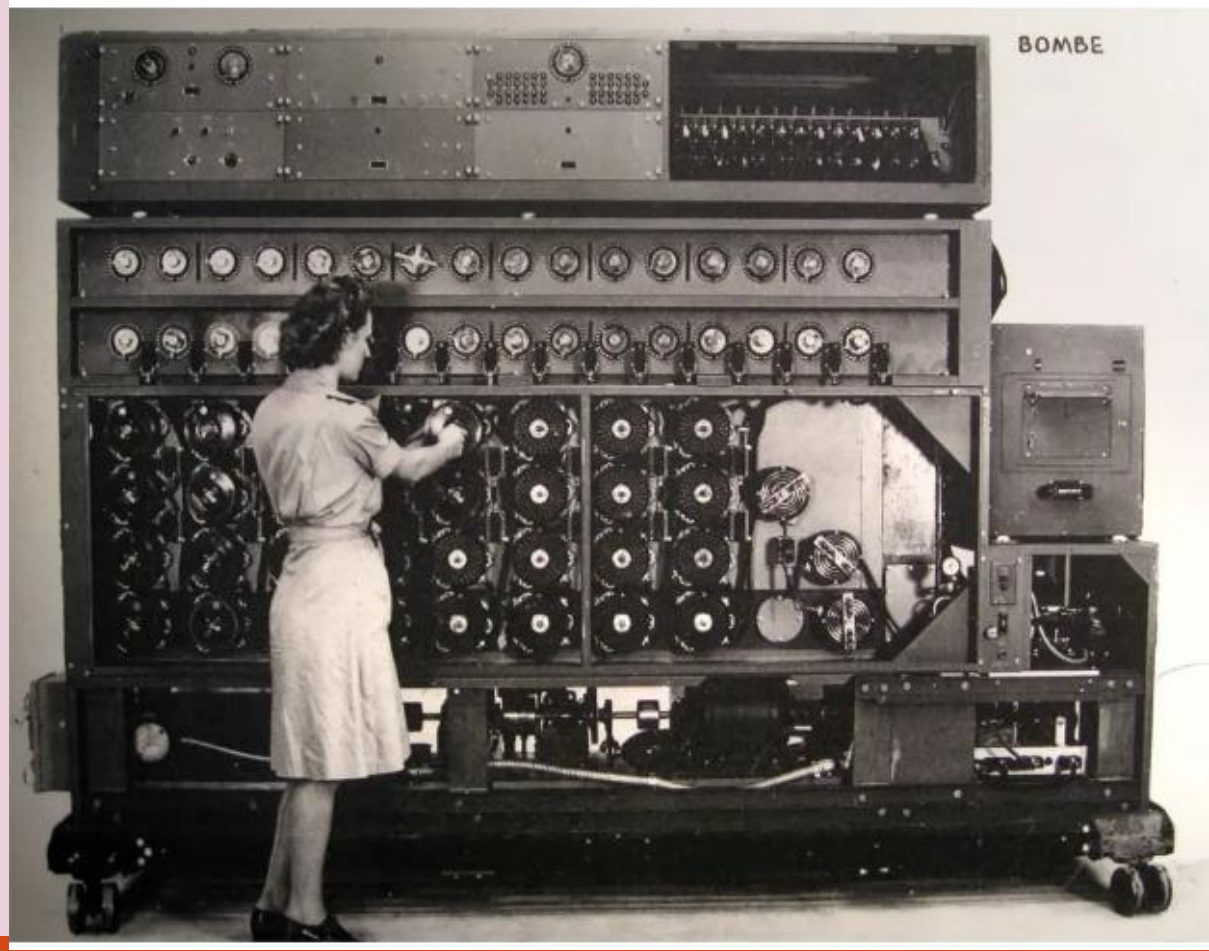


2 pav. Enigmos aparato su apgrąžos rotoriumi veikimo schema

- Vokiečių „Enigma“ elektromechaninė šifravimo mašina naudojo kintamąjį šifrą, keičiamą beveik kiekvieną dieną, todėl retai šifruotos karinės žinutės turėdavo tą patį šifravimo kodą.

- Enigma galėjo naudotis apie 159 milijonais milijonų milijonų įmanomų raktų.
- Į Enigma panašios šifravimo mašinos buvo naudojamos maždaug iki 1975 m., tik tada jas pakeitė elektroniniai kompiuteriai.
- Turingo išradimas - „Bombe“ mašina, kuri žymiai padidino perimtų vokiečių pranešimų dekodavimo greitį, yra Lenkijos matematikų darbo tęsinys.

daugiau čia



Filmas ENIGMA (liet.)

Keitinių šifrai: Postūmio šifras (*Shift Cipher*)

- Tai Cezario šifro apibendrinimas.
- **Veikimas**. Perstumti abėcėlėje ne per 3 raides, kaip Cezario šifro atveju, o per K raidžių, kur K yra šifro raktas, $0 < K < N$ (čia N yra abėcėlės raidžių skaičius).
- **Kriptoanalizė**. Ar gali kriptoanalitikas rasti raktą K?
  - TAIP! Brutalios jėgos ataka. Per maža raktų aibė!

Vienos abėcėlės keitinių šifrai (*Monoalphabetic Substitution Ciphers*) (1)

- **Raktai**: visi abėcėlės $\Sigma = \{A, B, C, \ldots, Z\}$ keitiniai.
- **Šifravimas** raktu π:
  - kiekviena pradinio teksto raidė X pakeičiama į $\pi(X)$.
- **Dešifravimas** raktu π:
  - kiekviena šifruoto teksto raidė Y pakeičiama į $\pi^{-1}(Y)$.
- **Pavyzdys**:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
π=	B	A	D	C	Z	H	W	Y	G	O	Q	X	S	V	T	R	N	M	S	K	J	I	P	F	E	U

TAIP $\rightarrow$ KBGR

Vienos abėcėlės keitinių šifrai (2)

- Brutalios jėgos ataka neįgyvendinama be šiuolaikinių kompiuterių, nes, pavyzdžiui, jei abėcėlėje yra N=26 raidės, tai skirtingų raktų yra 26! $\approx 4 \times 10^{26}$.
- Dominuoja slapto rašto mene pirmąjį mūsų eros tūkstantmetį.
- Tada daugelio laikytas neįveikiamu.

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 (2)

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) mod 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

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

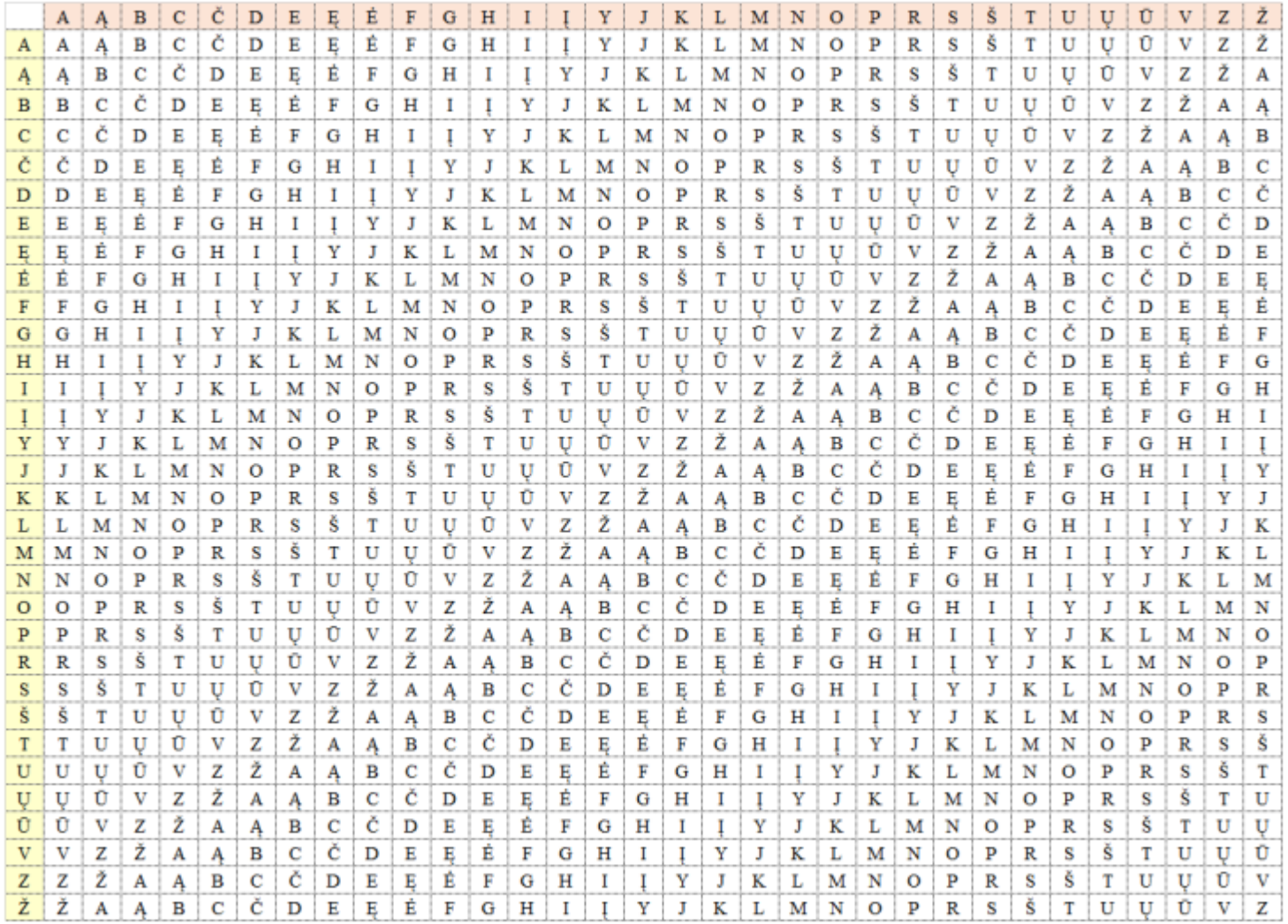
K	O	D	A	S	K	O	D	A	S	K	O	D	A	S
A	U	T	O	S	T	E	R	E	O	G	R	A	M	A
K	Y	Z	O	Y	F	U	Ų	E	H	U	G	D	M	S

Viženero šifras (3)

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.

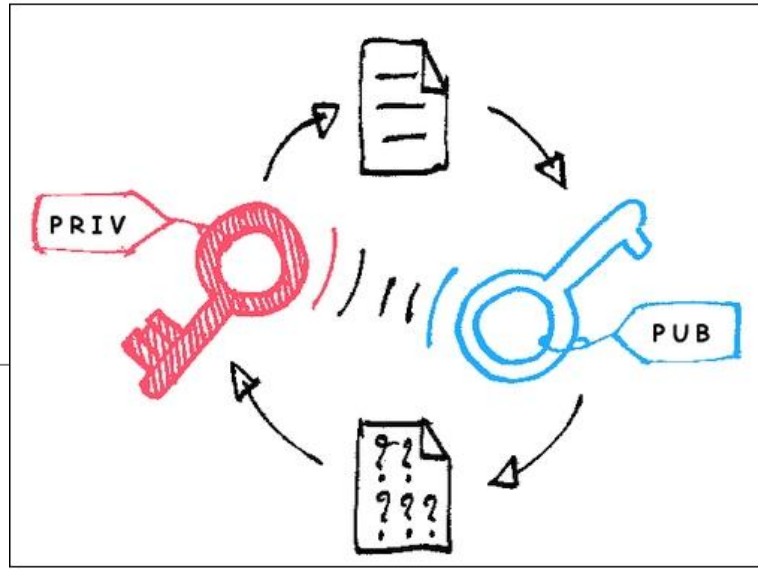
Lentelėje pateikiami 32 skirtingi Cezario šifrai



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

Viešojo rakto kriptosistemos

1976 metais Diffie ir Hellman pasiūlė naujo tipo kriptografiją, kurioje *šifravimo ir dešifravimo raktai yra skirtingi*.



- Vienas raktas yra viešai žinomas, kitas – saugomas slaptai.
- Klasikinėje kriptografijoje siuntėjas ir gavėjas turi bendrą raktą
- Viešojo rakto kriptografijoje – ne.
- Jei šifravimo raktas yra viešas, norint nusiųsti slaptą žinutę, tiesiog reikia užšifruoti ją su gavėjo viešuoju raktu.
- Gavėjas gali ją dešifruoti naudodamas savo privatųjį raktą.

Asimetrinis ir simetrinis šifravimas

- Asimetriškas reiškia kažką, kas nėra simetriška ar subalansuota.
- Kriptografijos kontekste **asimetrinis** šifravimas yra šifravimo tipas, kuriame ***naudojami du skirtingi raktai:*** vienas šifravimui ir kitas iššifravimui.
- Tai taip pat žinoma kaip viešojo rakto kriptografija, *kai vienas raktas yra viešas ir gali būti bendrinamas su bet kuo, o kitas raktas yra privatus savininkas.*
- Asimetrinis šifravimas dažniausiai *naudojamas saugiuose ryšio protokoluose*, tokiuose kaip SSL/TLS ir SSH.
- Ši technika *užtikrina aukštesnį saugumo lygį,* nes savininkas privatųjį raktą laiko paslaptyje.

Labai aukšto lygio SSH ir SSL yra technologijos, padedančios užšifruoti ir autentifikuoti duomenis, perduodamus tarp dviejų kompiuterių (pvz., nešiojamojo kompiuterio ir svetainės serverio).

Iš esmės **jie daro viską daug saugesnį.**

- **SSL** yra protokolas, kuris pirmiausia skirtas apsaugoti duomenų perdavimą *tarp dviejų šalių naudojant šifravimą ir autentifikavimą*. Dažniausiai šis perdavimas vyksta tarp kieno nors žiniatinklio naršyklės ir svetainės, kurioje jie lankosi, serverio.

- **SSH** siūlo saugų būdą *nuotoliniu* būdu prisijungti prie kito kompiuterio ir duoti komandas.

Daugiau skaityti čia

Asimetrinis ir simetrinis šifravimas

- ***Simetrinis*** šifravimas yra metodas, kai duomenims šifruoti ir iššifruoti ***naudojamas tas pats raktas***.
- Tai paprasta ir greita technika, tačiau ji turi reikšmingą *trūkumą*.
- Raktas turi būti *iš anksto pasidalytas* tarp siuntėjo ir gavėjo, todėl jis gali būti *perimtas* ir netinkamai naudojamas.

Už ir prieš

Simetrinis šifravimas turi keletą privalumų ir trūkumų.

Argumentai "už"

- Tai greitesnis ir efektyvesnis nei asimetrinis šifravimas.
- Jį lengviau įgyvendinti ir naudoti.
- Jis tinka šifruoti didelius duomenų kiekius.

Trūkumai

- Tam reikalingas saugus raktų keitimo būdas.
- Jis yra pažeidžiamas atakoms, jei slaptasis raktas yra pažeistas.
- Tai nesuteikia autentifikavimo ar neatmetimo.

Apskritai simetriškas šifravimas yra naudingas šifravimo būdas tam tikroms programoms, pvz., šifruojant didelius duomenų kiekius.

Tačiau prieš naudojant simetrinį šifravimą svarbu atidžiai apsvarstyti saugumo pasekmes ir apribojimus.

Už ir prieš

Asimetrinis šifravimas turi keletą privalumų ir trūkumų.

Argumentai "už"

- Saugesnis nei simetriškas šifravimas
- Viešuoju raktu galima dalytis nepažeidžiant saugumo
- Leidžia skaitmeniniais parašais patikrinti autentiškumą

Trūkumai

- Lėtesnis nei simetriškas šifravimas
- Sudėtingesnis įgyvendinimas ir valdymas
- Reikia daugiau apdorojimo galios nei simetriniam šifravimui

Apskritai asimetrinis šifravimas yra galingas įrankis duomenims apsaugoti ir pranešimų autentiškumui užtikrinti.

Nors jis gali būti lėtesnis ir sudėtingesnis nei simetriškas šifravimas, dėl papildomų saugumo privalumų jis yra vertingas įrankis bet kuriai organizacijai, norinčiai apsaugoti neskelbtiną informaciją.

Asimetrinė kriptografija

Asimetrinės kriptografijos pradžia galima laikyti 1976 m., kai du JAV mokslininkai Diffie'is ir Hellmanas publikavo savo garsųjį darbą „Naujos kriptografijos kryptys“, kuriame pirmą kartą buvo pasiūlytas, atrodytų sveikam protui prieštaraujantis algoritmas, kaip du nepažįstami žmonės, visiems girdint, gali bendrauti slaptai.

2013 m. vyko teismas tarp kompanijų „TQP Development“ ir „Newegg“. Pirmoji kompanija, spaudoje vadinama patentų troliu, padavė į teismą antrąją už jos patento pažeidimą. 1989 m. pateiktas patentas aprašo asimetrinės kriptografijos algoritmų kombinaciją, kuri tuo metų buvo akivaizdi, bei ne kartą aprašyta kriptografijos vadovėliuose. Į teismą kaip ekspertas liudyti buvo iškviestas pats Whitfieldas Diffie'is. Tarp teisėjo ir Diffie'io įvyko maždaug toks dialogas:

```
    – Šiame teismo procese mes daug girdėjome apie asimetrinę kriptografiją.
Ar jūs esate su ja susipažinęs?
    – Taip, esu.
    – Kaip gerai jūs esate su ja susipažinęs? – teisėjas uždavė
 patikslinantį klausimą.
    – Aš ją sukūriau, – atsakė Diffie'is.
```

Deja, nors Diffie'is ir liudijo prieš patentų trolį, teikdamas, kad jų patentas aprašo tai, kas tuo metu jau buvo ne kartą aprašyta net vadovėliuose, kompanija „Newegg“ teismo procesą pralaimėjo.

Daugiau apie simetrinį ir asimetrinį šifravimą skaitykite čia

Apie Enigmą čia (angl.)

RSA šifras (1)

RSA (Rivest–Shamir–Adleman abreviatūra) – viešojo rakto kriptosistema, kurios algoritmą 1977 metais sukūrė Ronald Rivest, Adi Shamir ir Leonard Adleman.

RSA metodu šifruojami skaičiai, o ne tekstas.

RSA yra kėlimo laipsniu šifras.

RSA šifras (2)

RSA metodo etapai:

1) pasirenkami du pakankamai dideli pirminiai skaičius p ir q;
2) skaičiuojamos tokios sandaugas: $n = p \times q$ ir $k = (p - 1) \times (q - 1)$;
3) pasirenkamas viešasis raktas (angl. *public key*) e, kuris neturi jokio bendro daugiklio, išskyrus 1 su skaičiumi k;
4) randamas toks privatusis raktas d (private key), kad $(d \times e) \bmod k = 1$. Šis raktas laikomas paslaptyje;
5) jei pasirenkame skaičių m, kurį norime užšifruoti, tai atliekamas toks veiksmas: skaičius keliamas k-uoju laipsniu ir skaičiuojama gauto skaičiaus liekana, kuri gaunama, tą skaičių operacija mod dalijant iš n: $c = m^e \bmod n$;
6) norint užšifruotą skaičių c iššifruoti, skaičius c keliamas laipsniu d ir liekana, gauta dalijant c^d iš n yra skaičius m: $c^d \bmod n = m$.

RSA šifras (3)

Pavyzdys

1) pasirenkame pirminius skaičius $p = 7$ ir $q = 13$. *(Tikri RSA pirminiai skaičiai turi būti bent 512 bitų ilgio, taip gaunant bent 1024 bitų ilgio n);*

2) randame sandaugas: $n = p \times q = 7 \times 13 = 91$ ir

$$k = (p - 1) \times (q - 1) = (7 - 1) \times (13 - 1) = 72;$$

3) pasirenkame viešąjį raktą $e = 5$, kuris neturi jokio bendro daugiklio, išskyrus 1, su skaičiumi $k = 72$;

4) randame privatųjį raktą

$d = 29$, kad $(d \times e) \bmod k = (29 \times 5) \bmod 72 = 145 \bmod 72 = 1$;

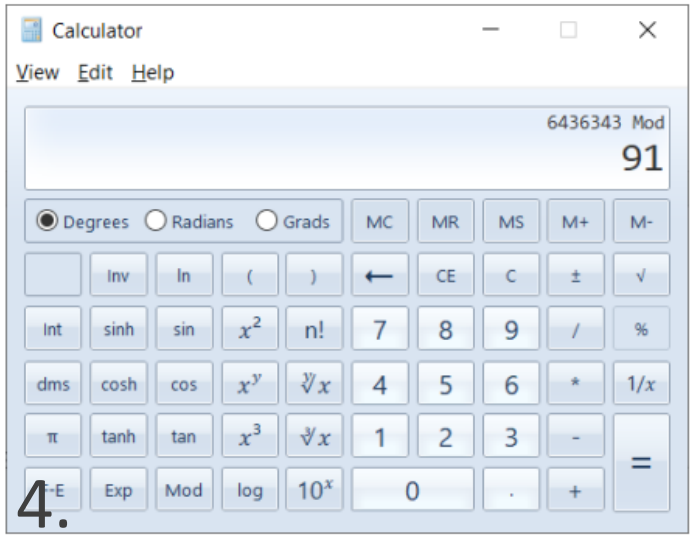
RSA šifras (4)

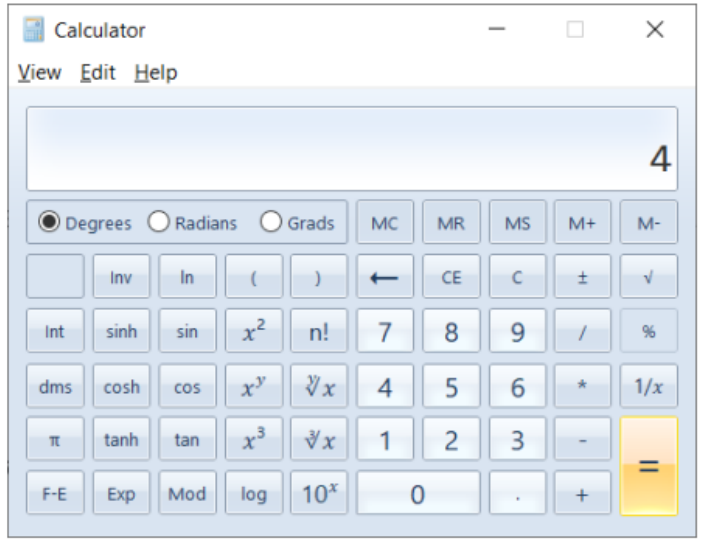
5) pasirenkame skaičių $m = 23$, kurį norime užšifruoti.

Pasirinktą skaičių 23 dalijame operacija mod iš n:

$$c = m^e \bmod n = 23^5 \bmod 91.$$

Veiksmus atliekame pasinaudodami skaičiuotuvu: 6436343 mod 91 = 4.





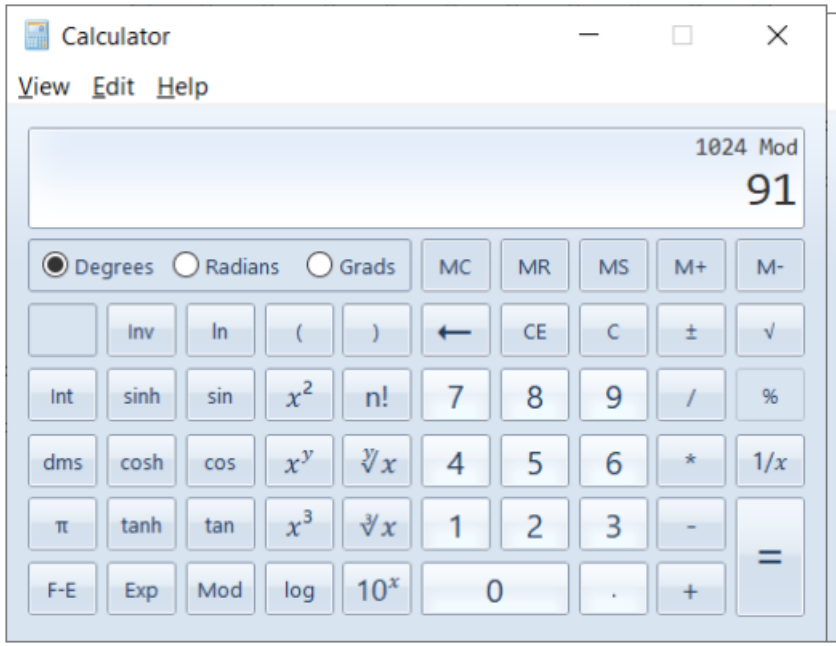
Skaičių 23 užšifravome ir gavome 4.

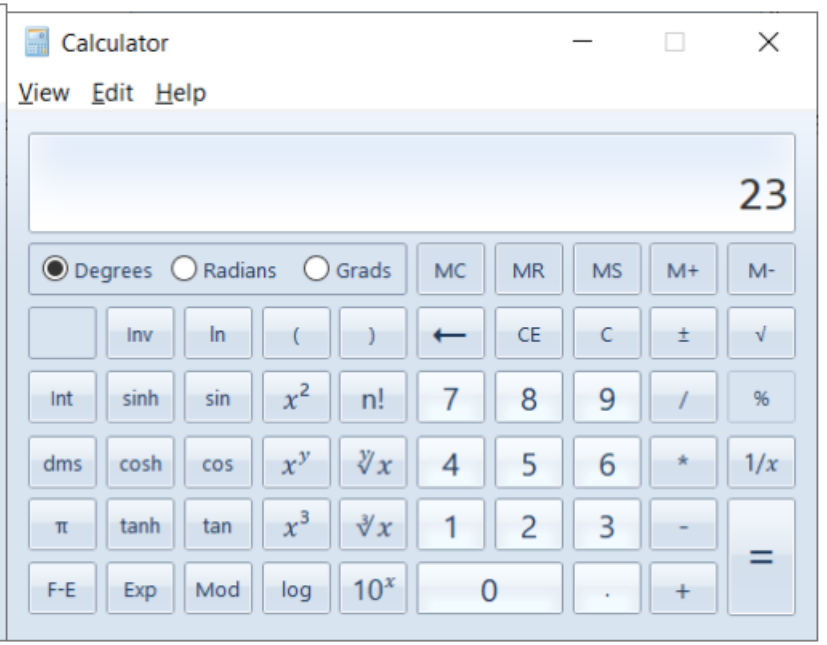
RSA šifras (5)

6) iššifruokime skaičių $c = 4$.

Skaičius $c = 4$ keliamas laipsniu $d = 5$ ir liekana, gauta dalijant 4^5 iš 91 yra skaičius $m = 23$:

$$c^d \bmod n = 4^5 \bmod 91 = 1024 \bmod 91 = 23.$$





RSA šifras (6)

Užduotis

Tegul $p = 5$ ir $q = 11$, viešasis raktas yra 3, o privatus – 27 (įsitikinkite, kad teisingai pasirinkti raktai).

Užšifruokite skaičių 18 ir įsitikinkite, kad teisingai užšfravote, jį iššifruodami.

Atsakymas

2

Teksto šifravimo RSA šifru pavyzdys (1)

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

Tarkime, kad $p = 7$, $q = 11$. Tada $n = 77$ ir $k = (7 - 1)(11 - 1) = 60$.

Viešais raktas tegul bus $e = 17$,
o privatų raktą galime apskaičiuoti, kad ir „Excel“ programa:

d	17d	17d mod 60
3	51	51
13	221	41
23	391	31
33	561	21
43	731	11
53	901	1
63	1071	51
73	1241	41
83	1411	31
93	1581	21
103	1751	11
113	1921	1
123	2091	51
133	2261	41
143	2431	31

Atlikus kelis skaičiavimus matome du tinkamus rezultatus.

Kad būtų paprasčiau, pasirenkame
mažesnį tinkamą raktą $d = 53$.

Teksto šifravimo RSA šifru pavyzdys (2)

Siuntėjas siunčia tokį pranešimą: TEISINGUMO LENTELĖ

T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08

Panaudojus viešąjį raktą $e = 17$ kiekvienam raidės numeriui $c = m^{17} \bmod 77$, gaunamas toks užšifruotas tekstas:

09 41 45 67 45 24 54 38 72 48 65 19 41 24 09 41 19 57

T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08
09	41	45	67	45	24	54	38	72	48	65	19	41	24	09	41	19	57

Teksto šifravimo RSA šifru pavyzdys (3)

Jei gavėjo privatus raktas $d = 53$, tai jis gautą užšifruotą pranešimą iššifruos taip: $m = c^{53} \bmod 77$

09	41	45	67	45	24	54	38	72	48	65	19	41	24	09	41	19	57
25	06	12	23	12	19	10	26	18	20	32	17	06	19	25	06	17	08
T	E	I	S	I	N	G	U	M	O		L	E	N	T	E	L	Ė

Teksto šifravimo RSA šifru pavyzdys (4)

Jei norima patvirtinti ir slaptumą, ir autentiškumą, reikia užšifruoti naudojant siuntėjo privatųjį raktą ir gavėjo viešąjį raktą.

Tegul siuntėjo viešasis raktas yra 17, o privatus – 53.

Gavėjo viešasis raktas yra 37, o privatus – 13.

Raidės T skaičius yra 25, todėl siuntėjas T raidę užšifruoja taip:

$(25^{53} \bmod 77)^{37} \bmod 77 = 58$.

Gavėjas naudoja savo privatųjį raktą 13, kad iššifruotų pranešimą, ir siuntėjo viešąjį raktą 17, kad įsitikintų jo autentiškumu: $(58^{13} \bmod 77)^{17} \bmod 77 = 25$.