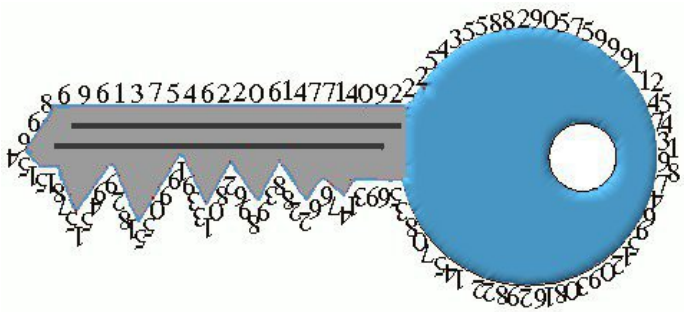
Kako zavarujemo skrivnosti pred starši?

Jernej Tonejc



UP IAM in Abelium d.o.o.

29. avgust 2013

O meni

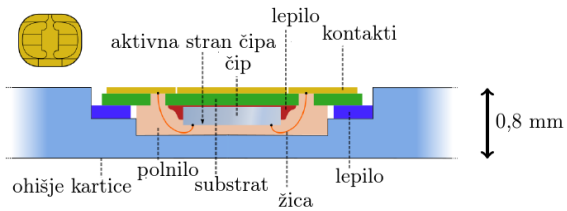
- Obiskoval ptujsko gimnazijo
- Tekmoval iz logike, matematike, kemije
- Dodiplomski študij matematike na FMF
- Podiplomski študij na FMF in UW-Madison
- Doktorat FMF 2007, UW-Madison 2008
- Od jeseni 2012 na IAM in v podjetju Abelium

O meni

- S kriptografijo se ukvarjam od 2000 dalje
- Sodeloval sem pri več projektih:
  - M-Pay/Moneta



  - Varno vložišče
  - Pametne kartice za MORS



Načrt

- **Osnove in zgodovina tajnopisja**
- Simetrična kriptografija
- Kriptografija z javnimi ključi
- Eliptične krivulje

Kaj je tajnopisje?

- Iz grščine $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma + \gamma\rho\acute{\alpha}\varphi\varepsilon\iota\nu =$ kriptografija oz. tajnopisje
- Veda o komunikaciji v prisotnosti aktivnega napadalca
- Kriptologija ali kriptografija?
- Teorija in praksa o skrivanju informacij
- Čistopis, tajnopis, ključ, šifra
- Šifriranje ali kodiranje?

Glavni igralci

Anita

Glavni igralci

Anita

Bojan

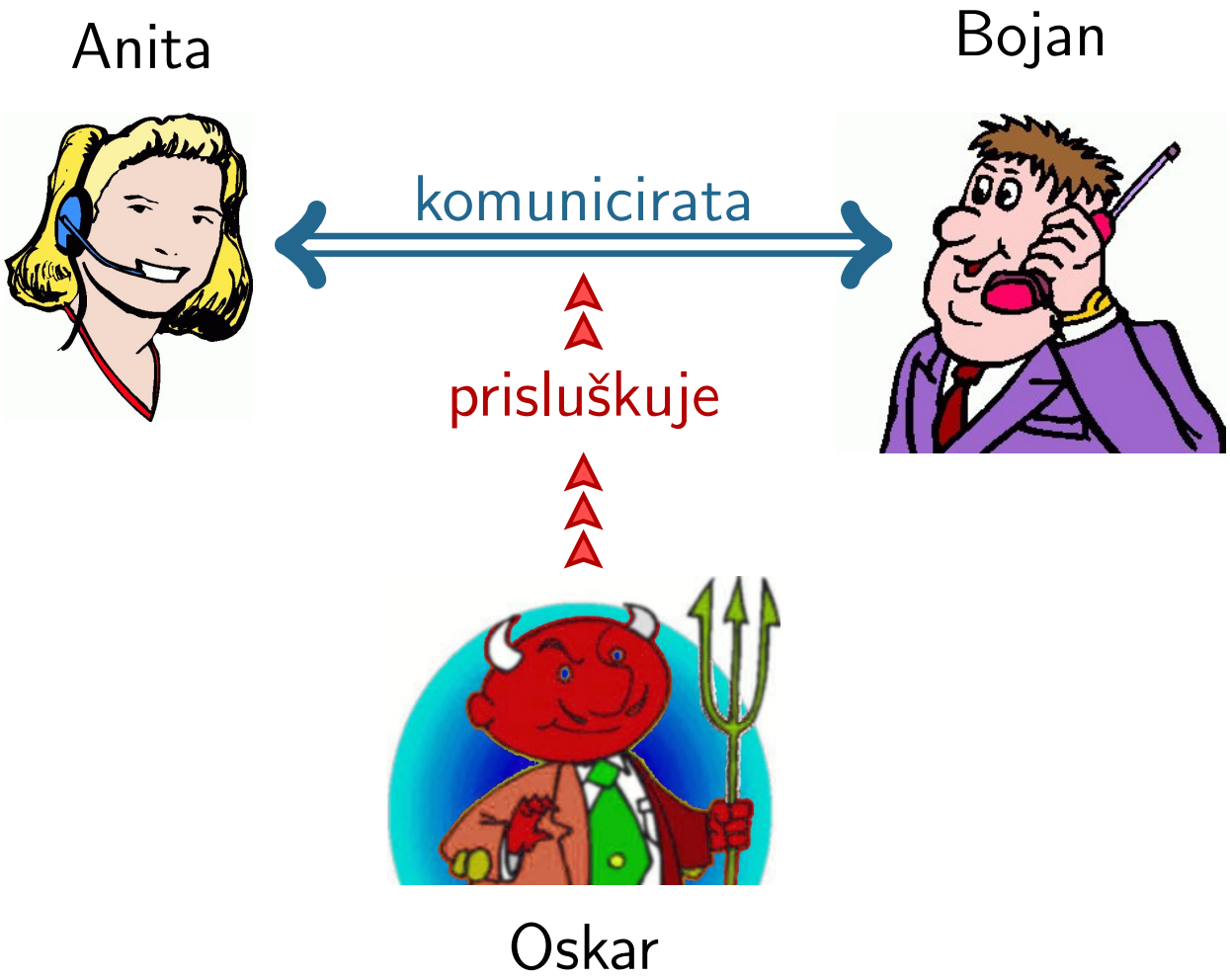
Glavni igralci

Anita

komunicirata

Bojan

Glavni igralci



Osnovni cilji kriptografije

- **Zaupnost**: ohraniti tajnost pred nepooblaščenimi.
- **Celovitost**: zagotoviti, da informacija ni bila spremenjena.
- **Verodostojnost**: potrditi izvor informacije.
- **Pristnost**: potrditi identiteto.
- **Preprečitev zatajitve**: preprečiti neizpolnitev sprejetih obvez ali dejanj.

Primer: pošiljanje običajnih dokumentov po pošti

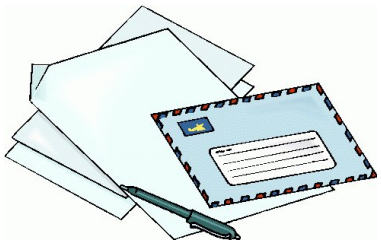
Kakšna zagotovila varnosti imamo? Kako?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura

Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Kako?

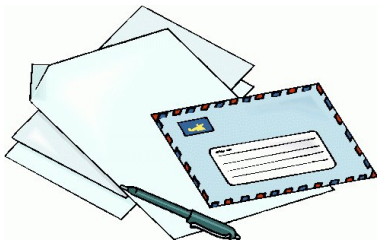
- Fizična varnost
- Zakonodaja
- Poštna infrastruktura



Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Kako?

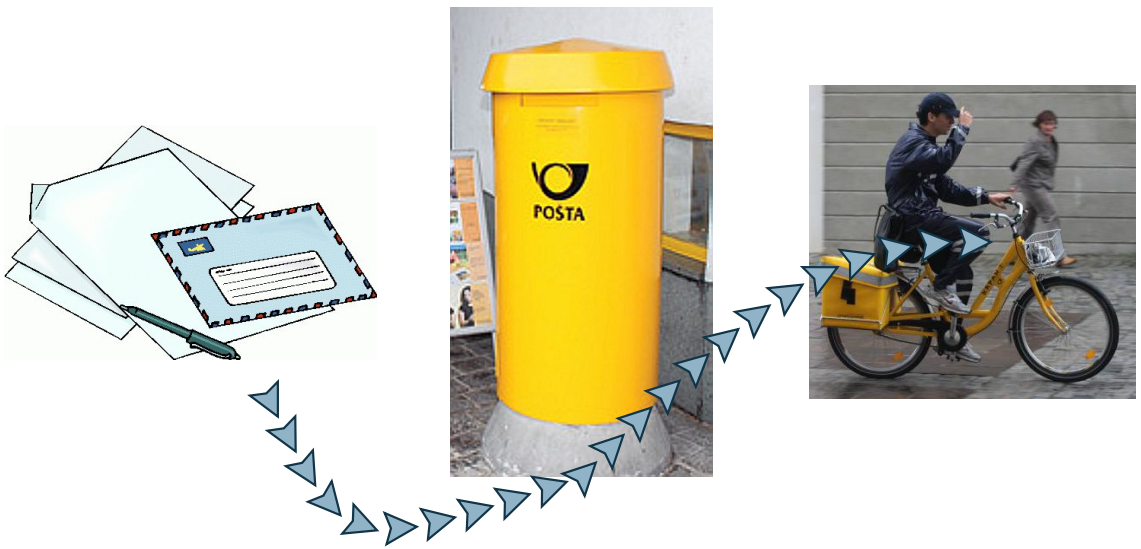
- Fizična varnost
- Zakonodaja
- Poštna infrastruktura



Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Kako?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura



Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Kako?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura

Primer: elektronski podatki

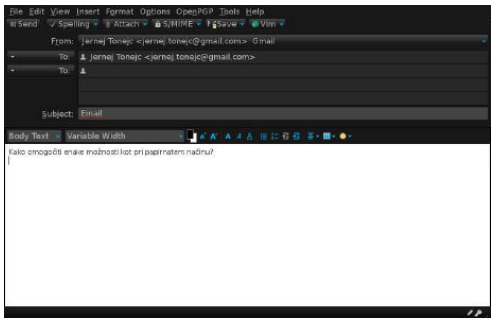
Kako omogočiti enake možnosti kot pri papirju?

- $+$ Enostavno in poceni hranjenje
- $+$ Hitro in enostavno prenašanje
- $-$ Enostavno kopiranje
- $-$ Prenosi niso (nujno) varni

Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirju?

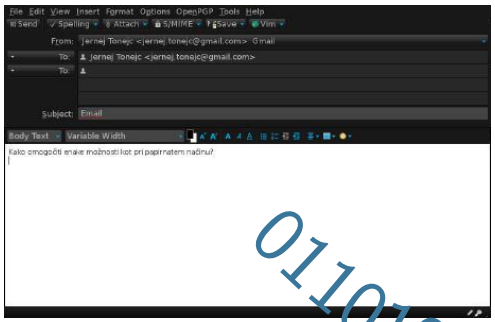
- $+$ Enostavno in poceni hranjenje
- $+$ Hitro in enostavno prenašanje
- $-$ Enostavno kopiranje
- $-$ Prenosi niso (nujno) varni

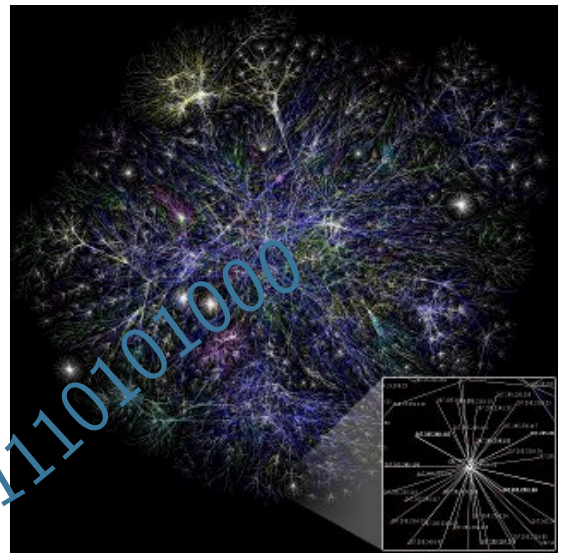


Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirju?

- \+ Enostavno in poceni hranjenje
- \+ Hitro in enostavno prenašanje
- − Enostavno kopiranje
- − Prenosi niso (nujno) varni

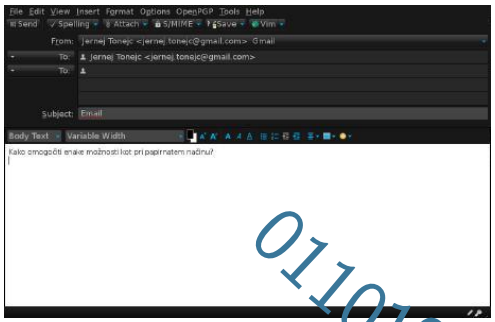


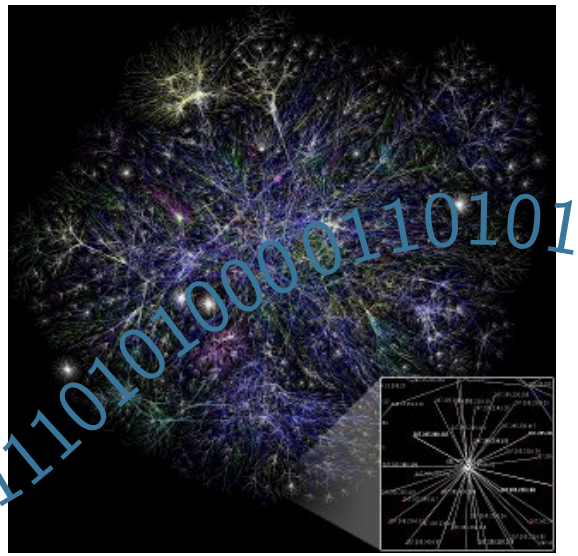


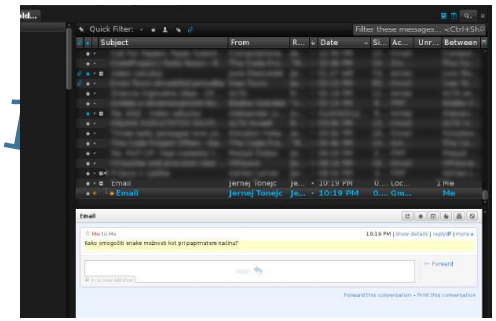
Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirju?

- \+ Enostavno in poceni hranjenje
- \+ Hitro in enostavno prenašanje
- − Enostavno kopiranje
- − Prenosi niso (nujno) varni







Začetki

- Najstarejši znani tajnopisi v Egiptu (∼ 2500 pr.n.št.)

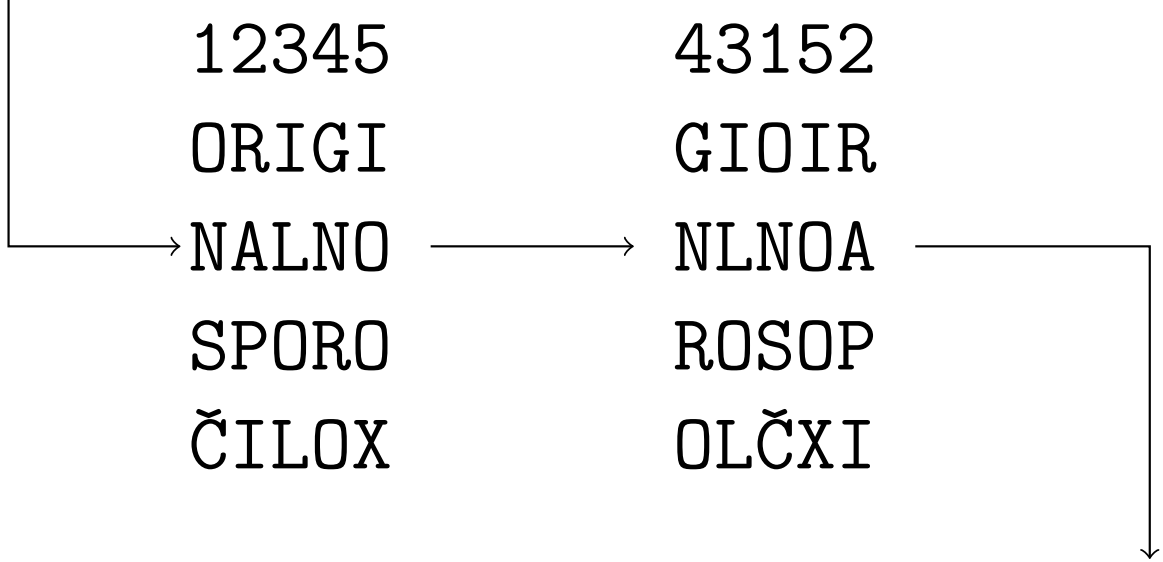
- Lončene tablice iz Mezopotamije z zašifriranimi recepti
- Preproste enoabecedne šifre pri Hebrejcih (∼ 600 pr.n.št.)
- Antika: skytale - palica

Transpozicijska šifra

- Črke originalnega sporočila ostanejo nespremenjene, njihova mesta pa so pomešana
- Zlahka prepoznamo, če izračunamo gostoto samoglasnikov ($\sim 41\%$ v slovenščini)
- Primer: Skytale

Primer: permutacija stolpcev

Originalno sporočilo



GioirnInoarosopolčxi

- Osnove in zgodovina tajnopisja
- **Simetrična kriptografija**
- Kriptografija z javnimi ključi
- Eliptične krivulje

Osnovne lastnosti

- Najstarejša oblika kriptografije
- Vse do Diffie-Hellmanove objave leta 1976 edina javno znana oblika
- Poznavanje enega ključa omogoča tako šifriranje kot dešifriranje sporočil $\Rightarrow$ simetrija
- V praksi dosega visoke hitrosti (procesor na mojem prenosniku zmore 3.9GB/s)

Lastnosti na primeru

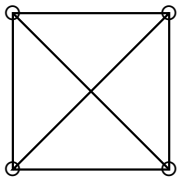
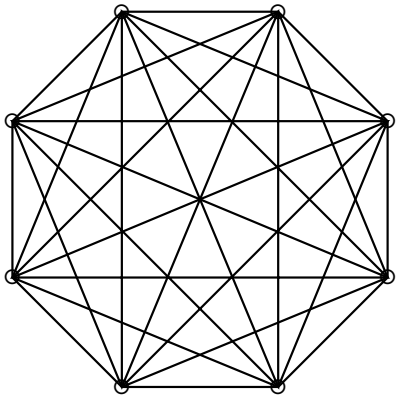
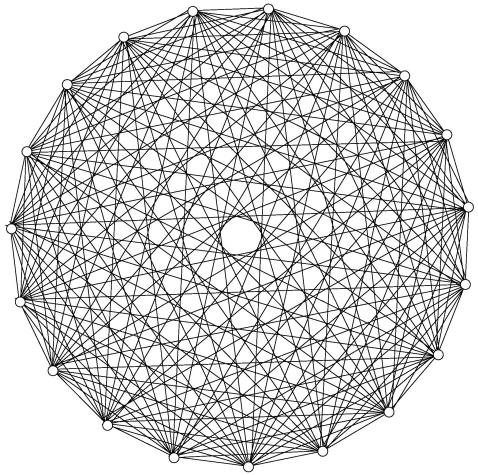
Bojan in Anita se vnaprej dogovorita za skupni ključ, ki ga ne pozna nihče drug. S tem ključem lahko tako zašifrirata kot dešifrirata sporočila.

Če Bojan z njim zašifrira pismo, je lahko prepričan, da ga lahko dešifrira le Anita.

Hkrati pa je tudi Anita zadovoljna, saj je prepričana, da ji je pismo lahko poslal le Bojan.

Problemi

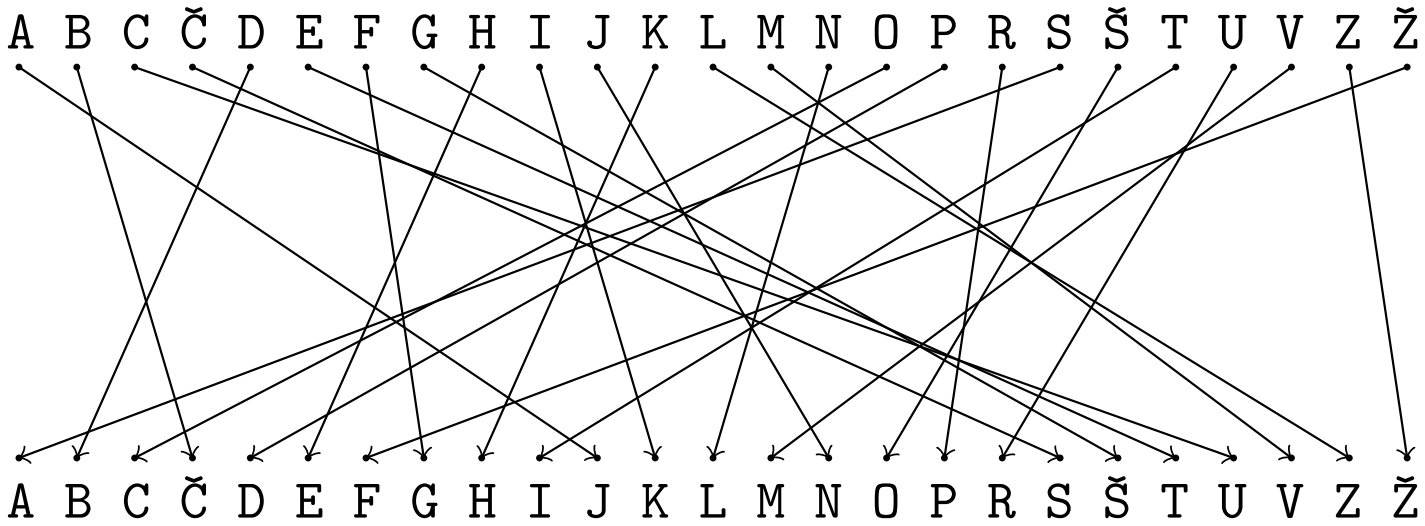
- Skupen ključ mora biti dogovorjen VNAPREJ.
- V omrežju z n uporabniki je potrebnih $\binom{n}{2}$ različnih ključev, vsak uporabnik pa mora hraniti $n-1$ ključev.

- Če se napadalec nekako dokoplje do ključa, lahko prebere VSA sporočila, ki smo jih kdajkoli zašifrirali.

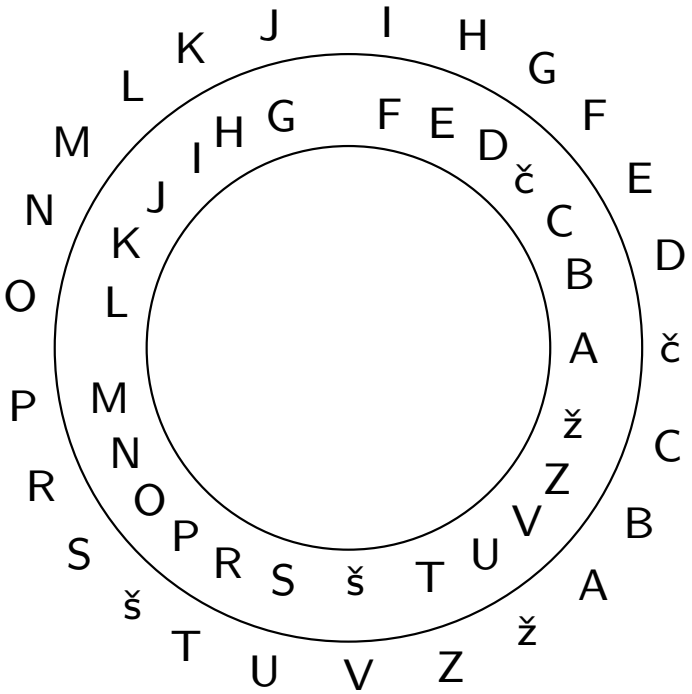
Zamenjalna (substitucijska) šifra

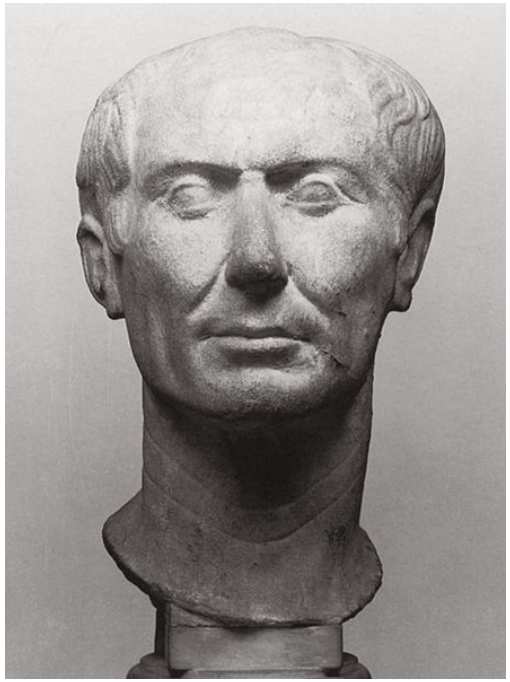
- Črke originalnega sporočila na enoličen način zamenjamo z drugimi simboli
- Če uporabimo kar isto abecedo, gre za permutacijo
- Relativno varna, če so sporočila kratka



Pomična šifra

- Poseben primer zamenjalne šifre
- Črke krožno zamaknemo. Julij Cezar: 3





- Primer: “Cezar” $\longrightarrow$ “Ehbčt”

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A B C Č D E F G H I J K L M N O P R S Š T U V Z Ž

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M									

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M	A								

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M	A	T							

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M	A	T	E						

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

```
A B C Č D E F G H I J K L M N O P R S Š T U V Z Ž
              M A T E
```

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

```
A B C Č D E F G H I J K L M N O P R S Š T U V Z Ž
              M A T E I
```

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M	A	T	E	I	K				

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
															M	A	T	E	I	K	B			

Varnejši primer zamenjalne šifre

- Izberemo si ključno črko in ključno besedo
- Ta par predstavlja ključ oz. geslo
- Permutacijo definiramo tako, da od ključne črke dalje pišemo geslo brez ponavljanja črk, nato (ciklično) dodamo preostale črke
- Npr. `O` in `MATEMATIKA`:

A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
F	G	H	J	L	N	O	P	R	S	Š	U	V	Z	Ž	M	A	T	E	I	K	B	C	Č	D

Vigenèrjeva šifra (1586)

- Poliabecedna šifra
- *Le chiffre indéchiffrable*
- Ločila in presledke ponavadi izpustimo
- Geslo pišemo nad besedilom, ponavljamo
- Trenutna črka v geslu določa, katero vrstico tabele uporabimo

	A	B	C	Č	D	E	F	G	H	I	...
A	A	B	C	Č	D	E	F	G	H	I	...
B	B	C	Č	D	E	F	G	H	I	J	...
C	C	Č	D	E	F	G	H	I	J	K	...
Č	Č	D	E	F	G	H	I	J	K	L	...
D	D	E	F	G	H	I	J	K	L	M	...
E	E	F	G	H	I	J	K	L	M	N	...
F	F	G	H	I	J	K	L	M	N	O	...
G	G	H	I	J	K	L	M	N	O	P	...
H	H	I	J	K	L	M	N	O	P	R	...
I	I	J	K	L	M	N	O	P	R	S	...
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.

Varnost Vigenèrjeve šifre

- Za geslo dolžine m imamo 25^m možnih ključev
- Za $m = 5$ je $9,7 \times 10^6$ že preveliko za "peš"
- Za $m = 18$ je $1,5 \times 10^{25}$ preveč tudi za računalnik
- Šifra kljub temu ni varna, če je besedilo daljše od približno $20m$, saj lahko uporabimo *test Kasiskega*, *Friedmanov indeks sovpadanja* oz. analizo frekvence črk.

Primer

- Geslo "ŠIFRA"
- Čistopis "SKRIVNOST"

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo "ŠIFRA"
- Čistopis "SKRIVNOST"
- Š I F R A Š I F R
  S K R I V N O S T

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo "ŠIFRA"
- Čistopis "SKRIVNOST"
- Š I F R A Š I F R
  S K R I V N O S T

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo "ŠIFRA"
- Čistopis "SKRIVNOST"
- Š I F R A Š I F R
  S K R I V N O S T

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T

⇒ L

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  $\Rightarrow$ L
- Zašifriramo kot LTZBVHŽŽL

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  $\Rightarrow$ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  $\Rightarrow$ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”
- Š I F R A Š I F R
  L T Z B V H Ž Ž L

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  $\Rightarrow$ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”
- Š I F R A Š I F R
  L T Z B V H Ž Ž L

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  $\Rightarrow$ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”
- Š I F R A Š I F R
  L T Z B V H Ž Ž L

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
A	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
B	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
C	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
Č	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
Š	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
T	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
U	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
V	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
Z	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
Ž	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z

Primer

- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  ⇒ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”
- Š I F R A Š I F R
  L T Z B V H Ž Ž L
  ⇒ S

Primer

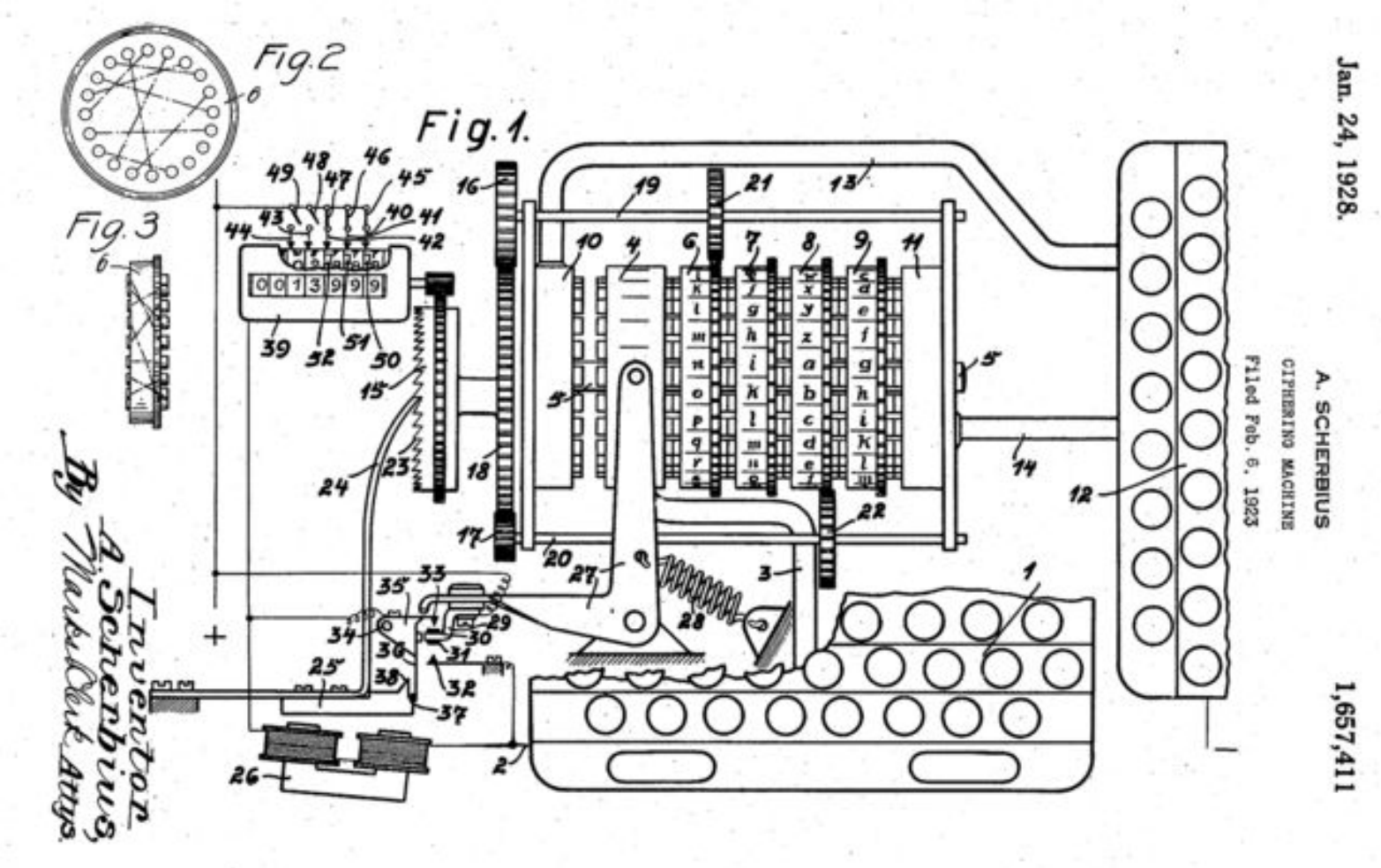
- Geslo “ŠIFRA”
- Čistopis “SKRIVNOST”
- Š I F R A Š I F R
  S K R I V N O S T
  ⇒ L
- Zašifriramo kot LTZBVHŽŽL
- Tajnopis “LTZBVHŽŽL”
- Š I F R A Š I F R
  L T Z B V H Ž Ž L
  ⇒ S
- Dešifriramo kot SKRIVNOST

Enigma

- Izumil Arthur Scherbius po 1. svetovni vojni
- Elektro-mehanična naprava s koluti
- Izdelanih več variant
- Na začetku trije koluti, kasneje do 8
- Glavna nemška šifrirna naprava pred in med 2. svetovno vojno
- Za razbijanje zgrajen prvi računalnik – Colossus I.

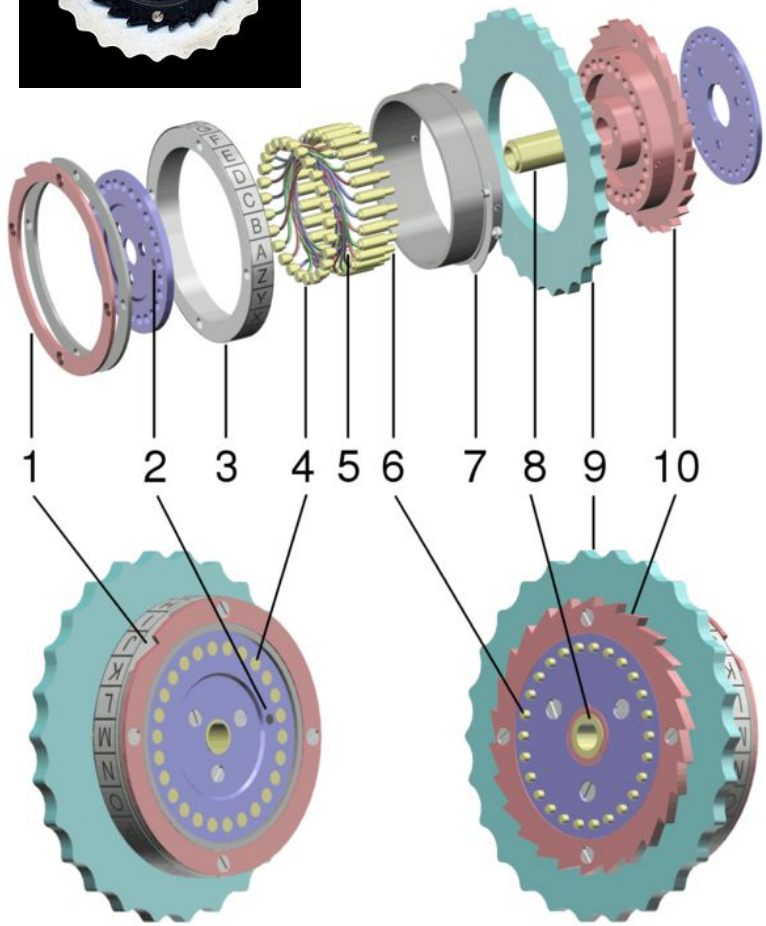
Simulacija na http://enigmaco.de/

Patent za Enigmo

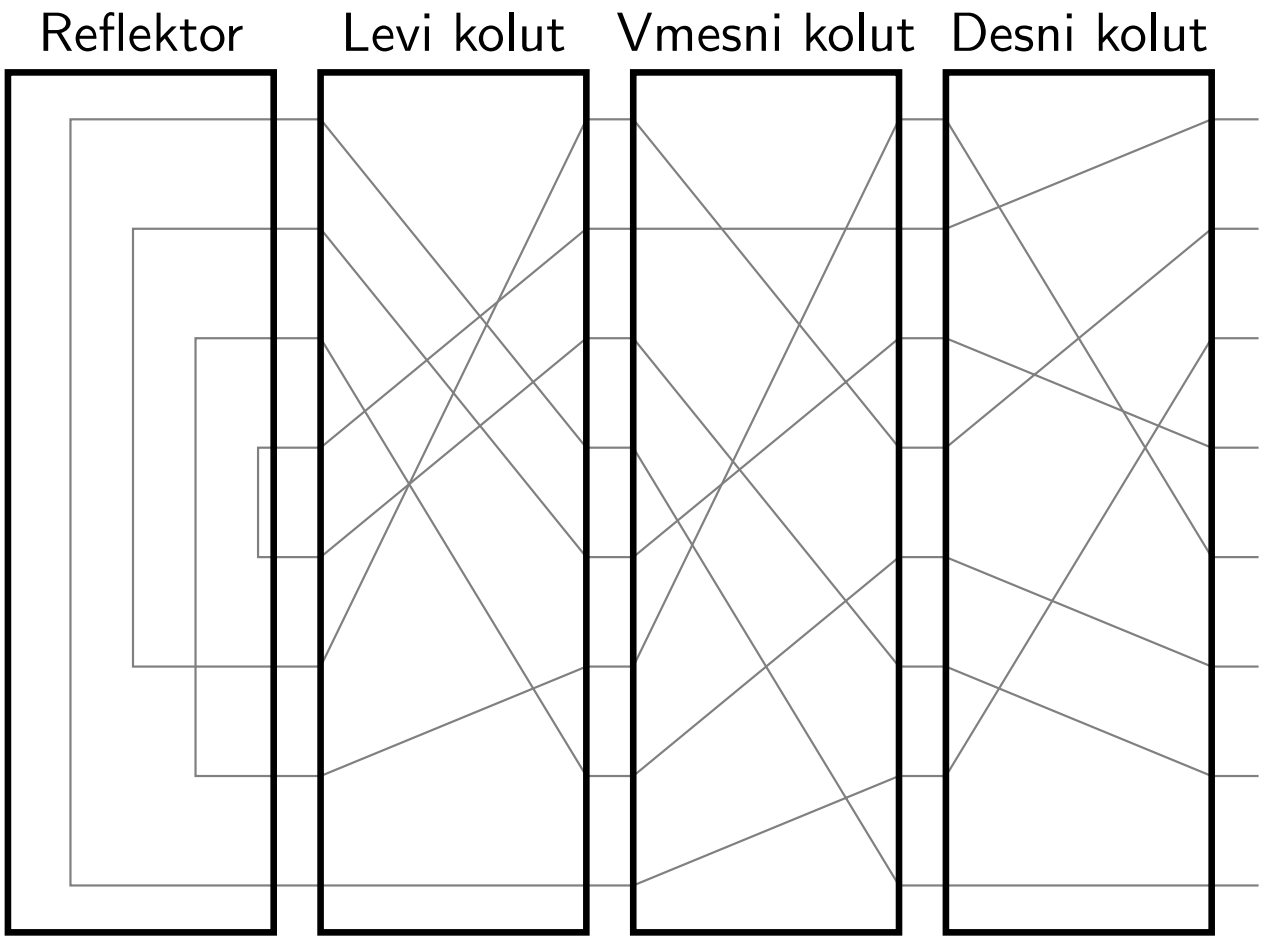


Zgradba kolutov

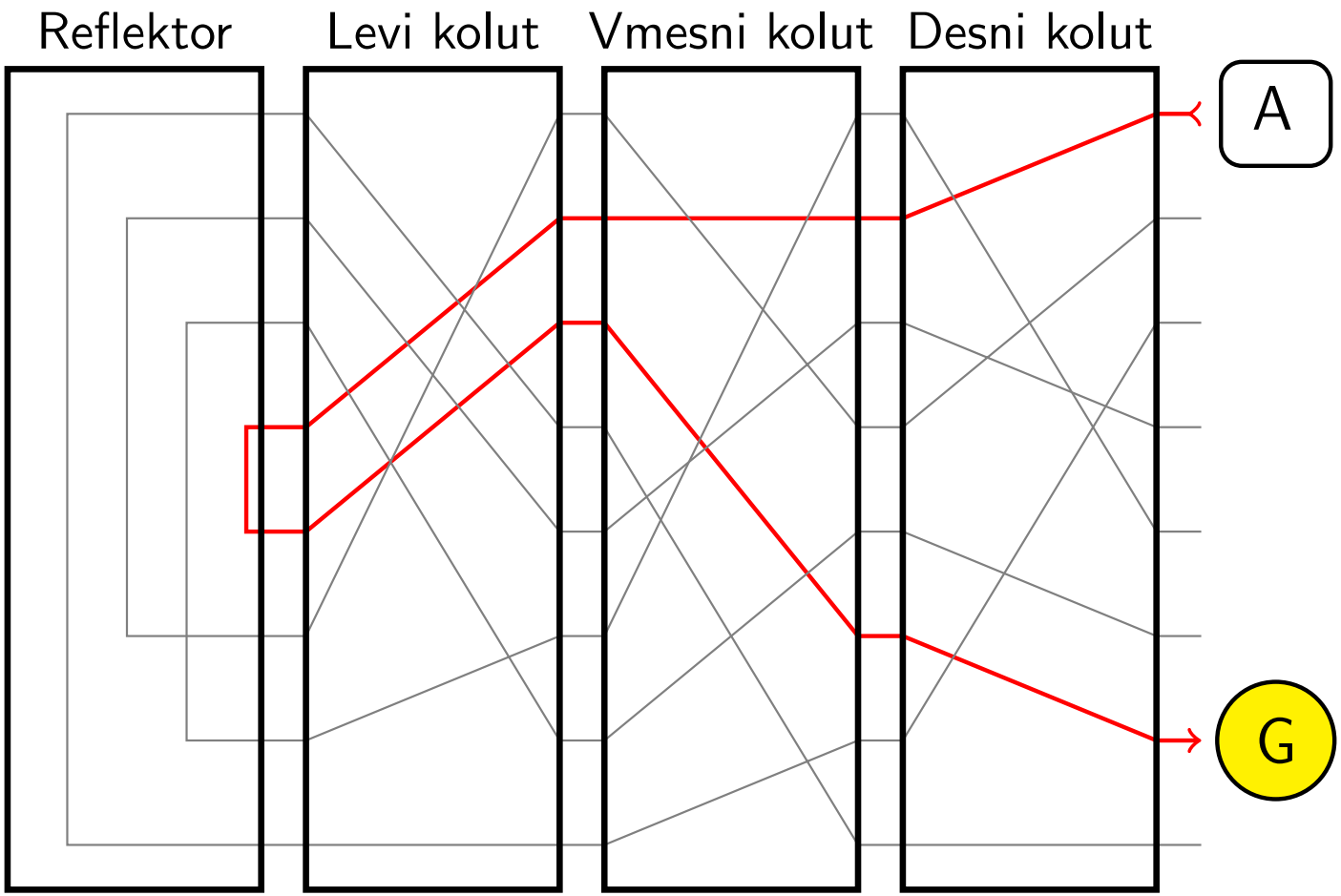
1. Obroč z utorom
2. Oznaka za 'A'
3. Obroč s črkami
4. Plošča s kontakti
5. Povezave
6. Zatiči s kontakti
7. Nastavitveni obroč
8. Os
9. Kolut za ročni pomik
10. Obroč z zarezami



Princip delovanja

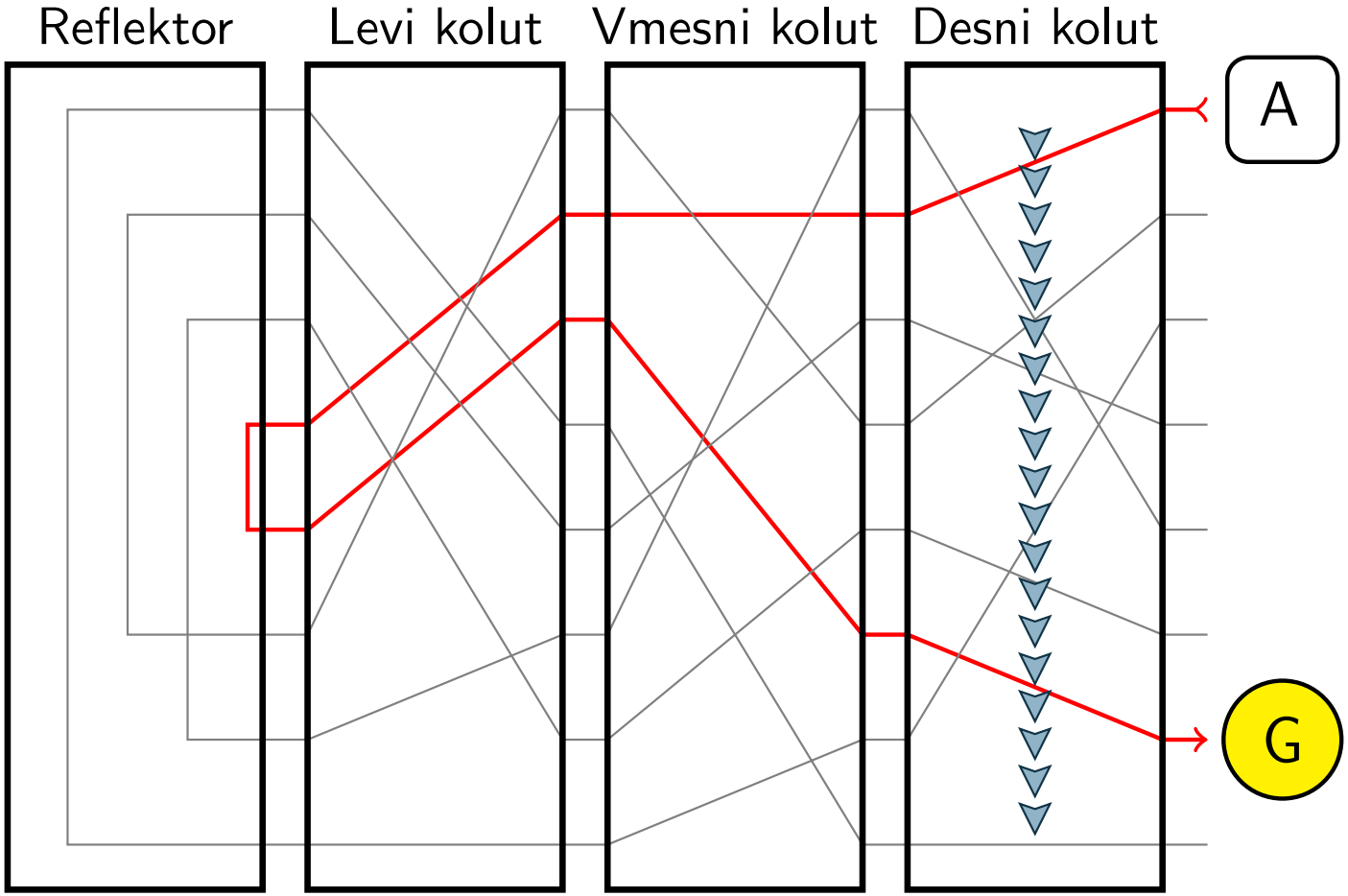


Princip delovanja

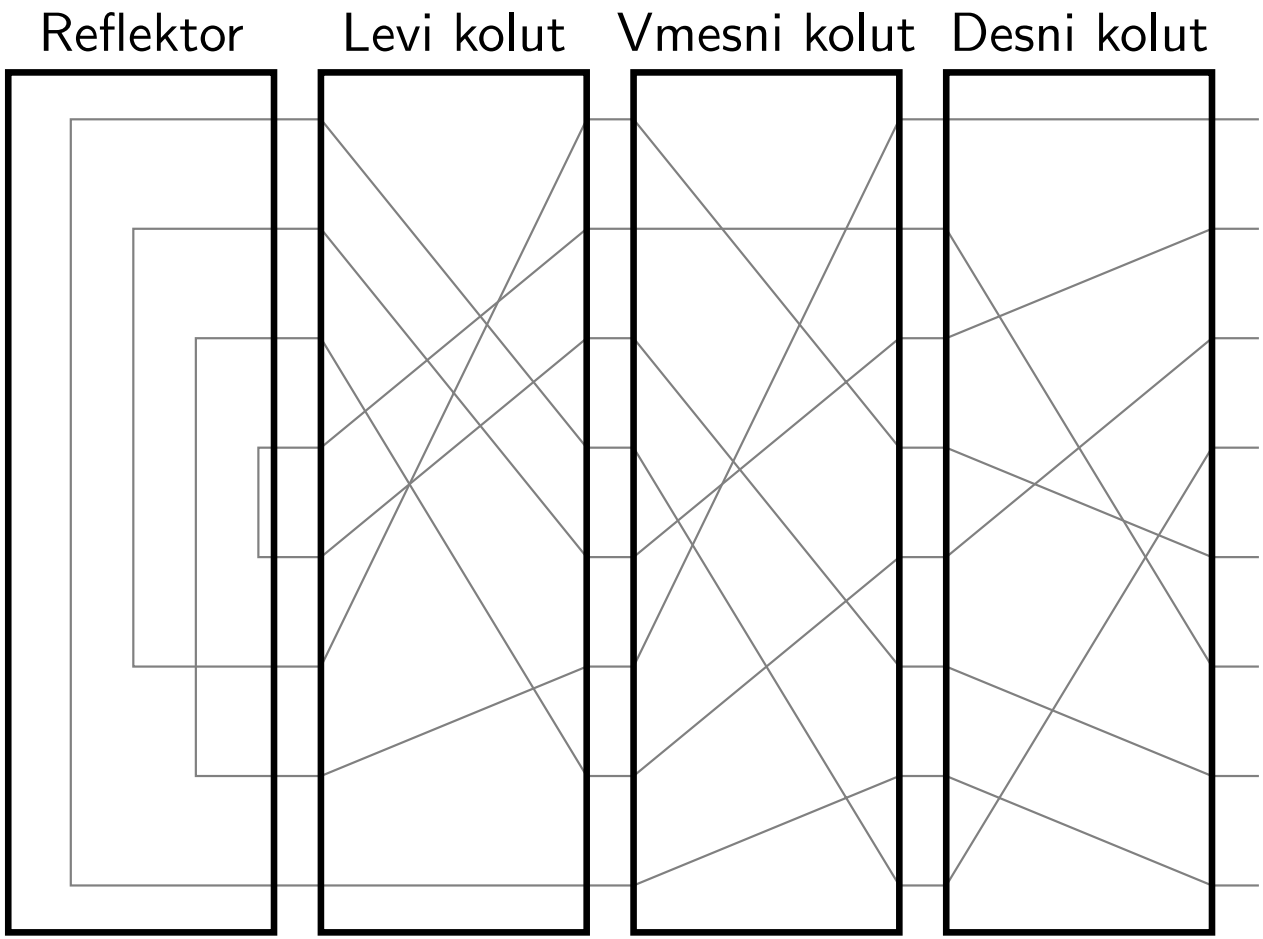


Princip delovanja

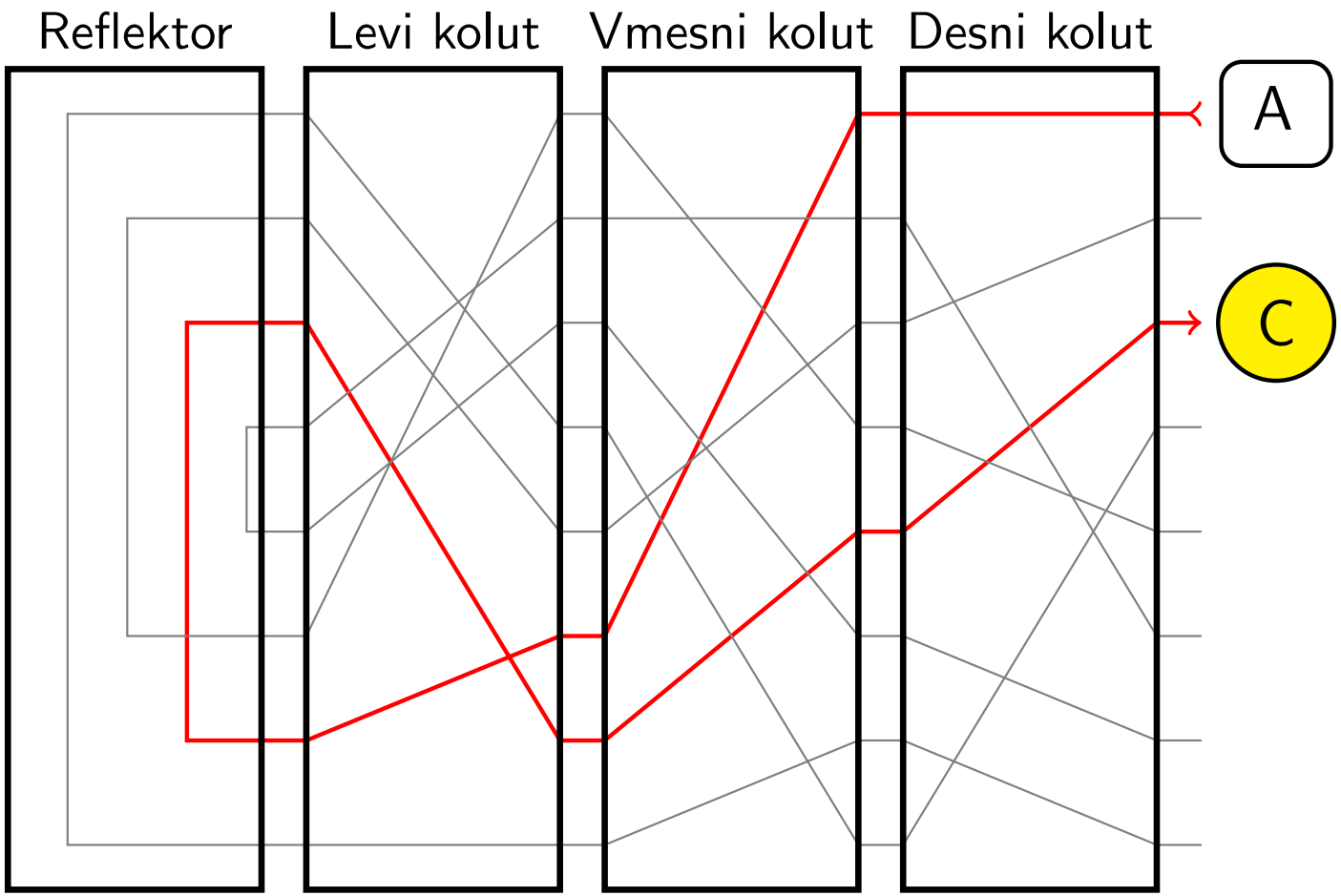
Po pritisku tipke se desni kolut pomakne za eno mesto.



Princip delovanja



Princip delovanja



Enigmin ključ

Nastavljeno enkrat dnevno:

- izbor kolutov (3 izmed 5) $\Rightarrow$ 10 možnosti
- izbor reflektorja (1 izmed 2)$\Rightarrow$ 2 možnosti
- vrstni red kolutov (3!) $\Rightarrow$ 6 možnosti
- notranje nastavitve kolutov $\Rightarrow$ 676 možnosti
- prevezave stikalne plošče $\Rightarrow$ 150738274937250 možnosti

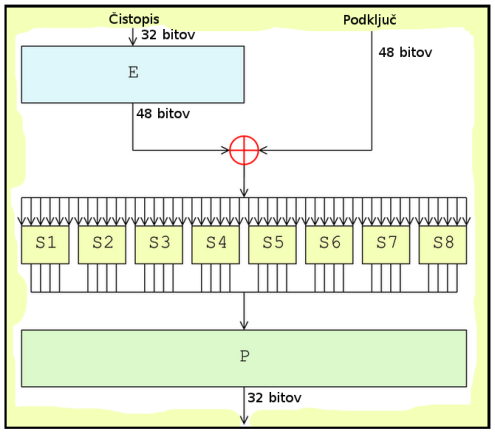
Nastavljeno za vsako sporočilo:

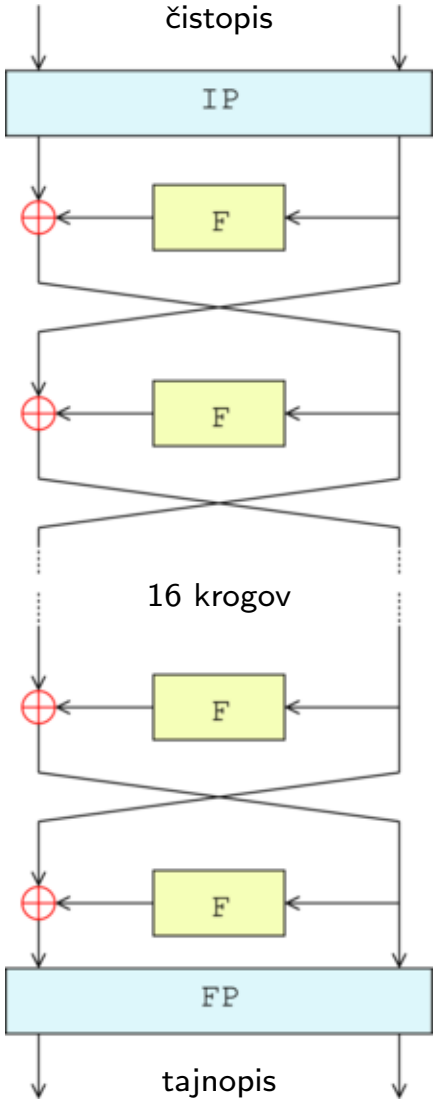
- začetni položaj kolutov $\Rightarrow$ 17576 možnosti

Skupaj približno $2{,}15 \times 10^{23}$ možnih ključev.

DES

- Data Encryption Standard
- 56 bitni ključ
- razvil IBM l. 1974 s pomočjo NSA[a]
- leta 1981 postane bančni standard
- konec 90-ih vse učinkovitejši napadi
- Funkcija F:

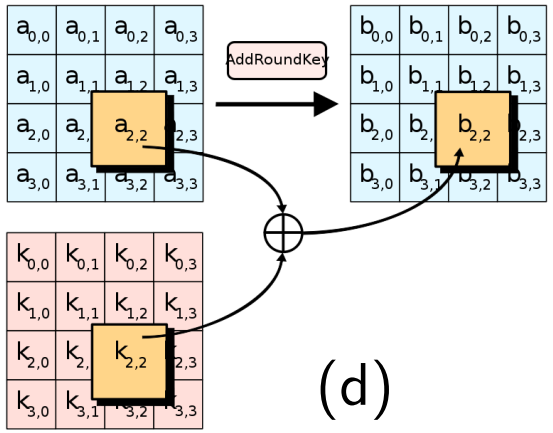


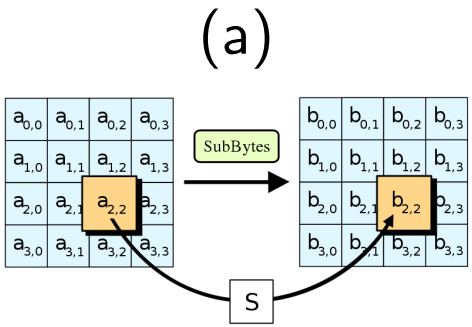


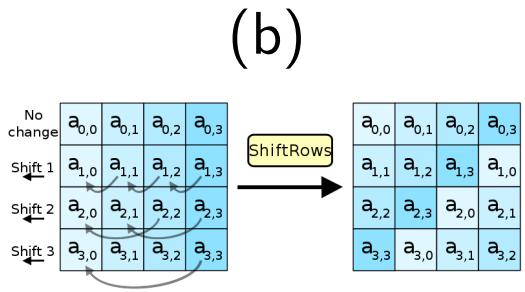
[a]National Security Agency

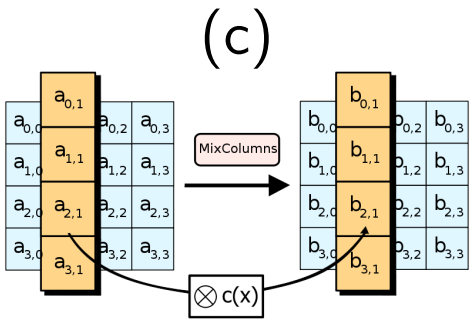
AES-128, -192, -256

- Advanced Encryption Standard
- Izbran na javnem razpisu NIST
- 1997 pričetek izbora
- 1999 izbranih 5 finalistov
- 2001 objavljen zmagovalec
- Zaporedje korakov:
  $\mathrm{d} \longrightarrow (\mathrm{a},\ \mathrm{b},\ \mathrm{c},\ \mathrm{d}) \times k \longrightarrow \mathrm{a},\ \mathrm{b},\ \mathrm{d}$









Načrt

- Osnove in zgodovina tajnopisja
- Simetrična kriptografija
- **Kriptografija z javnimi ključi**
- Eliptične krivulje

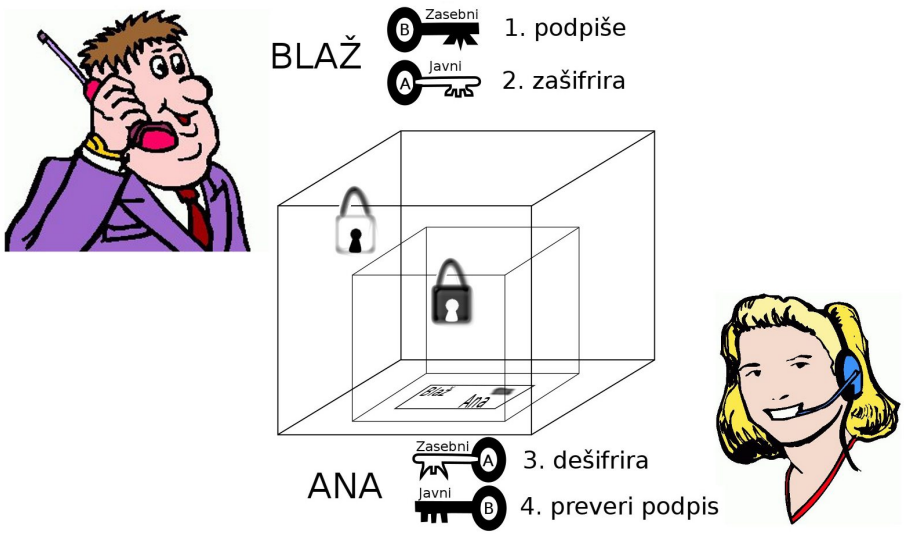
Osnove

- Leta 1976 Whit Diffie in Martin Hellman predstavita koncept kriptografije z javnimi ključi.
- Vsak uporabnik ima 2 ključa: en podatke zaklepa, drugi jih odklepa.
- Pomembno: ključ, ki zaklepa, ne more odklepati in obratno, ključ, ki odklepa, ne more zaklepati.
- En ključ lahko objavimo, drugega pa hranimo $\Rightarrow$ javni in zasebni ključ.

Primer

Bojan pošlje Aniti podpisano zasebno pismo:

- podpiše ga s svojim zasebnim ključem Z_B,
- zašifrira ga z Anitinim javnim ključem J_A.



- Anita ga s svojim zasebnim ključem Z_A dešifrira,
- z Bojanovim javnim ključem J_B pa preveri podpis.

Matematično ozadje

Sistemi javne kriptografije, se glede na matematični problem, na katerem temeljijo, delijo v tri skupine:

- Sistemi faktorizacije celih števil, npr. RSA (Rivest-Shamir-Adleman),
- Sistemi diskretnega logaritma, npr. DSA (Digital Signature Standard),
- Kriptosistemi z eliptičnimi krivuljami, ECC (Elliptic Curve Cryptography).

RSA

- Potrebujemo dve veliki naključno izbrani praštevili: p in q
- Produkt je enostavno izračunati: $n = pq$
- Faktorizirati n je težek problem
- Računamo po modulu n

RSA

- Šifrirni eksponent je število e, da velja* $\mathrm{D}(e, \varphi(n)) = 1$
- Dešifrirni eksponent je d, ki zadošča $ed \equiv 1 \pmod{\varphi(n)}$.
- Javni ključ je (n, e), zasebni pa d
- Šifriramo tako, da izračunamo $y = x^e \bmod n$
- Dešifriramo tako, da izračunamo $y^d \bmod n$

*φ je Eulerjeva funkcija

Problemi RSA

- Če znamo faktorizirati n, potem znamo iz e izračunati d
- Zaradi vse bolj učinkovitih algoritmov za faktorizacijo mora biti n vse večji – 512 bitov (155 mestno število) ni več dovolj, priporoča se vsaj 1024 bitov (309 mestno število).
- Počasen v primerjavi z drugimi kriptosistemi z javnimi ključi za isti nivo varnosti

Dolžina ključev

simetrične šifre (AES)	**asimetrične** (RSA, DSA)	**eliptične krivulje**
40 bitov	274 bitov	80 bitov
56 bitov	384 bitov	106 bitov
64 bitov	512 bitov	132 bitov
80 bitov	**1024 bitov**	**160 bitov**
96 bitov	1536 bitov	185 bitov
112 bitov	2048 bitov	237 bitov
120 bitov	2560 bitov	256 bitov
128 bitov	3072 bitov	270 bitov
256 bitov	15380 bitov	521 bitov

Napad z grobo silo

dolžina ključev (v bitih)	**število možnih ključev**	**potreben čas pri enem šifriranju/μs**	**potreben čas pri 10^6 šifriranjih/μs**
32	$2^{32} \approx 4,3 \times 10^9$	$2^{31}\mu$sek $\approx$ 36 min	$\approx$ 2ms
56	$2^{56} \approx 7,2 \times 10^{16}$	$\approx$ 1142 let	$\approx$ 10 ur
80	$2^{80} \approx 1,2 \times 10^{24}$	$\approx 1,9 \times 10^{10}$ let	$\approx 1,9 \times 10^4$ let
128	$2^{128} \approx 3,4 \times 10^{38}$	$\approx 5 \times 10^{24}$ let	$\approx 5 \times 10^{18}$ let

Za primerjavo: starost vesolja se ocenjuje na $13,7 \times 10^9$ let.

Načrt

- Osnove in zgodovina tajnopisja
- Simetrična kriptografija
- Kriptografija z javnimi ključi
- **Eliptične krivulje**

Modularna aritmetika

- Ostanek pri deljenju z **modulom** m
- Oznaka: $a \bmod m$. Velja $m \bmod m = 0$.
- Primer: ura. Ko pridemo do 12, nadaljujemo z 0.
- Operacije kot običajno. Če presežemo m, popravimo.
- Primer:

$$(3 + 6) \bmod 7 = 9 \bmod 7 = (7 + 2) \bmod 7 = 0 + 2 = 2$$
$$(3 \cdot 6) \bmod 7 = 18 \bmod 7 = (2 \cdot 7 + 4) \bmod 7 = 0 + 4 = 4$$

Osnove

Definicija

a deli b, $a \mid b$, če obstaja $k \in \mathbb{Z}$, da velja $b = ka$.

Definicija

Število p je praštevilo, če ima natanko dva različna delitelja, 1 in samega sebe.

Definicija

Največji skupni delitelj $\mathrm{D}(a, b)$ celih števil a in b je največje tako število $d \in \mathbb{Z}$, da velja $d \mid a$ in $d \mid b$.

Osnove, nadaljevanje

Definicija

Celi števili a in b sta si tuji, če velja $\mathrm{D}(a, b) = 1$.
Pišemo $a \perp b$.

Izrek (o deljivosti)

Za poljubni naravni števili a in b, $a \geqslant b$, obstajata $k, r \in \mathbb{N}$, $0 \leqslant r < b$, da velja $a = k \cdot b + r$.

Trditev

Za poljubne $a, b, c \in \mathbb{Z}$ velja $\mathrm{D}(a, b) = D(a - bc, b)$.

Evklidov algoritem

Izrek

Naslednji algoritem izračuna največji skupni delitelj danih naravnih števil a in b, $a \geqslant b$.

1. $r_{-1} = a$, $r_0 = b$
2. *Dokler je* $r_i \neq 0$, *izračunaj* $r_{i+1} = r_{i-1} - q_i r_i$, *kjer je* $q_i \in \mathbb{N}$ *in* $0 \leqslant r_{i+1} < r_i$.
3. *Če je* $r_n \neq 0$ *in* $r_{n+1} = 0$, *potem je* $\mathrm{D}(a, b) = r_n$.

Primer

- Naj bo $a = 85$, $b = 35$.
- Potem je $q_0 = \lfloor \frac{a}{b} \rfloor = 2$ in $r_1 = 15$.
- Podobno je $q_1 = \lfloor \frac{35}{15} \rfloor = 2$ in $r_2 = 5$.
- Nazadnje je $q_2 = \lfloor \frac{15}{5} \rfloor = 3$ in $r_3 = 0$.
- $\mathrm{D}(85, 35) = 5$

Linearne diofantske enačbe

Izrek

Za poljubna $a, b \in \mathbb{Z}$, *ne oba* 0, *ima enačba*

$$ax + by = c$$

rešitev natanko tedaj, ko $\mathrm{D}(a, b) \mid c$.

OPOMBA. Rešitev dobimo z razširjenim Evklidovim algoritmom.

Poseben primer je $c = 1$.

Kongruence

Definicija

Naj bo $m \in \mathbb{N}$. Celi števili a in b sta kongruentni po modulu m, z oznako $a \equiv b \pmod{m}$, če velja $m \mid a - b$.

Oznaka $x = a \bmod m$ pomeni, da a reduciramo po modulu m, rezultat x je število med 0 in $m - 1$.

Obsegi

Obseg je struktura, v kateri imamo:

- operaciji seštevanja $+$ in množenja $\cdot$
- elementa 0 in 1
- za vse a velja $a + 0 = 0 + a = a$
- za vse a velja $a \cdot 1 = 1 \cdot a = a$
- za vsak a obstaja $-a$, da velja $a + (-a) = 0$
- za vsak $a \neq 0$ obstaja a^{-1}, da velja[†] $a \cdot a^{-1} = 1$

Primer: realna števila, racionalna števila

[†]Inverz elementa. To je dejansko deljenje, $a/a = 1$

Praštevilski obsegi

Realna in racionalna števila niso primerna za računalnike. (Zakaj?) Zato v kriptografiji uporabljamo končne obsege.

- Naj bo p praštevilo
- Množica ostankov pri deljenju s p je obseg
- $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$
- Seštevanje, odštevanje, množenje po modulu
- Deljenje?

Primer: multiplikativna tabela za $p = 11$

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2		4	6	8	10	1	3	5	7	9
3			9	1	4	7	10	2	5	8
4				5	9	2	6	10	3	7
5					3	8	2	7	1	6
6						3	9	4	10	5
7							5	1	8	4
8								9	6	3
9									4	2
10										1

Vidimo, da lahko inverze preberemo iz tabele. Tako je npr. $5^{-1} = 9$, $8^{-1} = 7$.

Deljenje z razširjenim Evklidovim algoritmom

Za inverz a po modulu m v splošnem iščemo tak x, da velja

$$ax \bmod m = 1 \text{ oziroma, } ax \equiv 1 \pmod{m}.$$

Inverz obstaja, če je $\mathrm{D}(a, m) = 1$. To lepše zapišemo kot

$$ax + bm = 1$$

To pa je linearna diofantska enačba!

Kako rešiti linearno diofantsko enačbo

- Naj bo $\mathrm{D}(a, m) = 1$ in $m > a$.
- Iz a in m znamo dobiti $\mathrm{D}(a, m)$
- Oglejmo si

$$a \cdot 0 + m \cdot 1 = m$$
$$a \cdot 1 + m \cdot 0 = a$$

- Če izvajamo Evklidov algoritem na enačbah, po nekaj korakih pridemo do

$$a \cdot x + m \cdot b = 1$$

Primera

Naj bo $m = 17$, $a = 7$.

17	1	0
7	0	1
3	1	-2
1	-2	5

Torej je $-2 \cdot 17 + 5 \cdot 7 = 1$,
zato je $7^{-1} \bmod 17 = 5$.

Naj bo $m = 97$, $a = 17$.

97	1	0
17	0	1
12	1	-5
5	-1	6
2	3	-17
1	-7	40

Zato $17^{-1} \bmod 97 = 40$
$(40 \cdot 17 = 680 = 7 \cdot 97 + 1)$

Eliptične krivulje

- Za kriptografijo sta jih leta 1985 prva predlagala Neal Koblitz in Victor Miller
- Eliptična krivulja E je definirana z Weierstrassovo enačbo[‡]

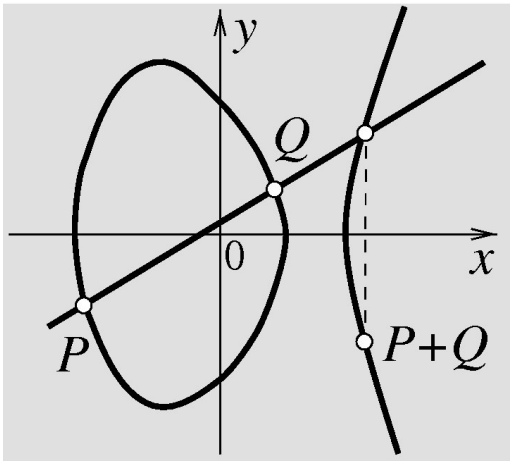
$$y^2 = x^3 + ax + b$$

- Gledamo množico točk (x, y), ki ustrezajo tej enačbi, skupaj s točko $\mathcal{O}$ v neskončnosti

[‡] poenostavljen primer

Pravilo za seštevanje

- Različni točki P in Q seštejemo tako, da skozi njiju potegnemo premico, nato pa tretje presečišče te premice s krivuljo prezrcalimo čez x-os:



- Če je $P = Q$, potem skozi P potegnemo *tangento*.

Seštevanje dveh različnih točk

- Vzemimo različni točki $P = (x_1, y_1)$ in $Q = (x_2, y_2)$ na eliptični krivulji $E : y^2 = x^3 + ax + b$
- Enačba premice skozi P in Q je

$$y = mx + n, \tag{1}$$

kjer je $m = \frac{y_2 - y_1}{x_2 - x_1}$ in $n = y_1 - mx_1 = y_2 - mx_2$

- Iz (1) vstavimo y v enačbo krivulje:

$$(mx + n)^2 = x^3 + ax + b$$

Seštevanje dveh različnih točk

- Preuredimo enačbo:

$$x^3 - m^2x^2 + (a - 2mn)x + b - n^2 = 0$$

- Dve ničli sta x_1 in x_2, vsota ničel je koeficient pri $-x^2$, torej m^2.
- Od tod dobimo $x_3 = m^2 - x_1 - x_2$
- Iz enačbe premice sledi še $y_3' = m(x_3 - x_1) + y_1$ in po prezrcaljenju $y_3 = m(x_1 - x_3) - y_1$

Podvajanje točke

- Za izračun $2P = P + P$ potrebujemo enačbo tangente na E skozi P
- Kot prej je $n = y_1 - mx_1$, ko enkrat imamo m
- Za m odvajamo enačbo krivulje:

$$2y\frac{dy}{dx} = 3x^2 + a$$

in upoštevamo $m = \frac{dy}{dx} = \frac{3x_1^2+a}{2y_1}$

Podvajanje točke

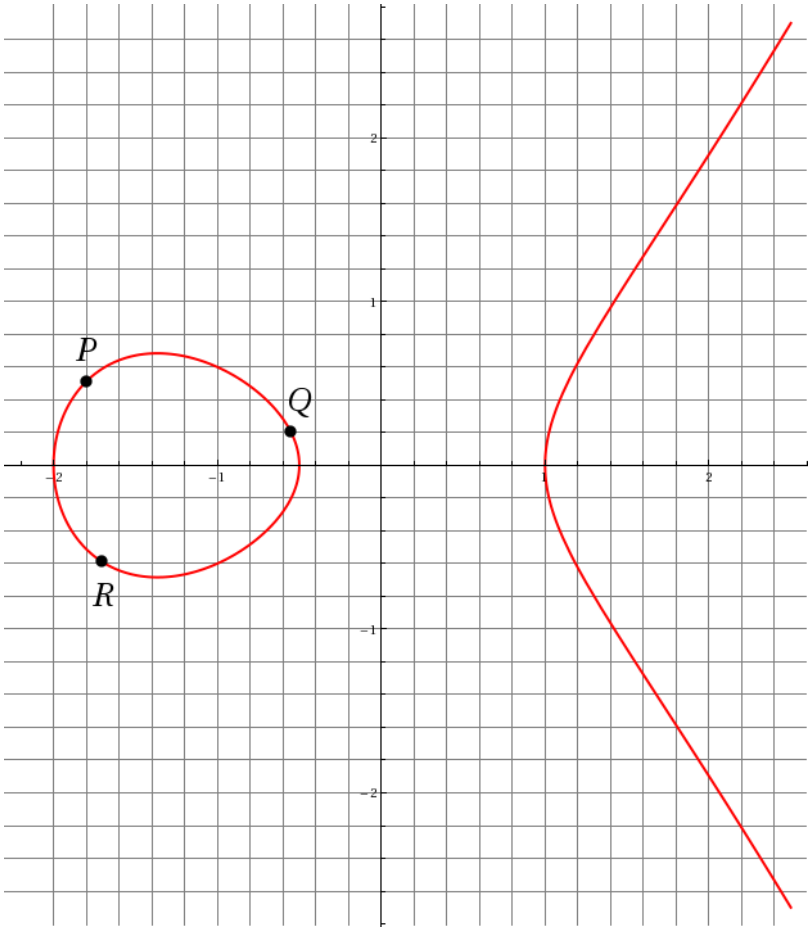
- Nadaljujemo kot prej, enačbo premice vstavimo v enačbo krivulje
- Tokrat sta dve ničli x_1, ki je dvojna
- Od tod dobimo $x_3 = m^2 - 2x_1$
- Iz enačbe premice sledi še $y_3' = m(x_3 - x_1) + y_1$ in po prezrcaljenju $y_3 = m(x_1 - x_3) - y_1$

Seštevanje točk - povzetek

- Če je $Q = \mathcal{O}$, je $P + Q = P$
- Če je $Q = -P$, je $P + Q = \mathcal{O}$
- Sicer pa je $P + Q = (x_3, y_3)$, kjer je

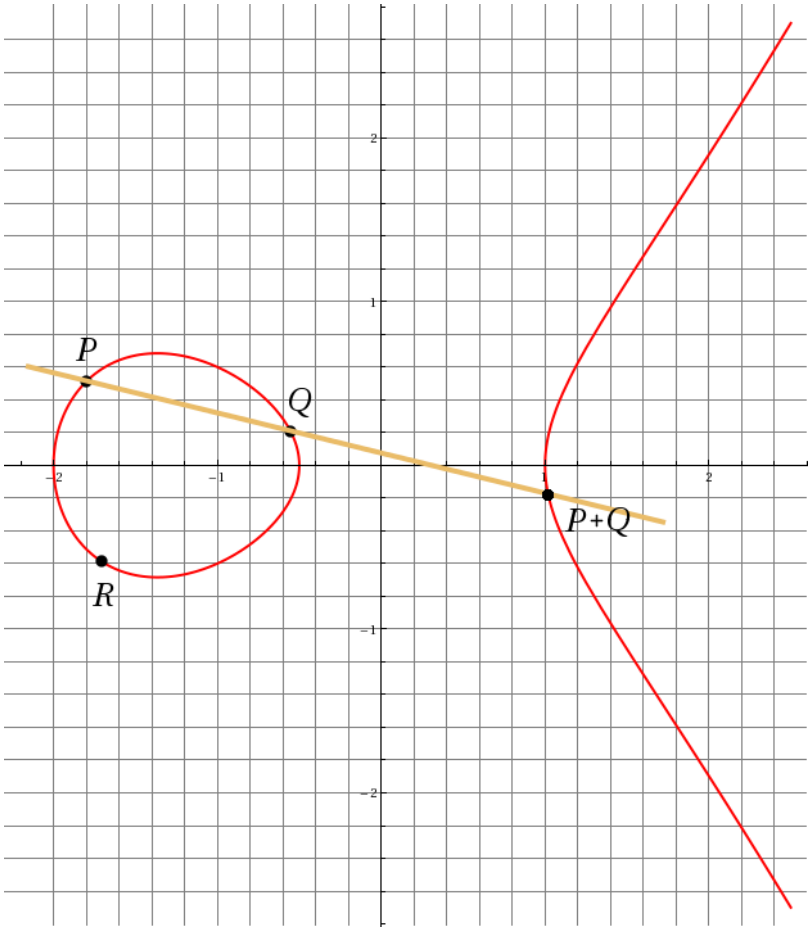
$$x_3 = m^2 - x_1 - x_2,$$
$$y_3 = m(x_1 - x_3) - y_1,$$
$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{če } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1}, & \text{če } P = Q \end{cases}$$

Zakaj prezrcalimo?



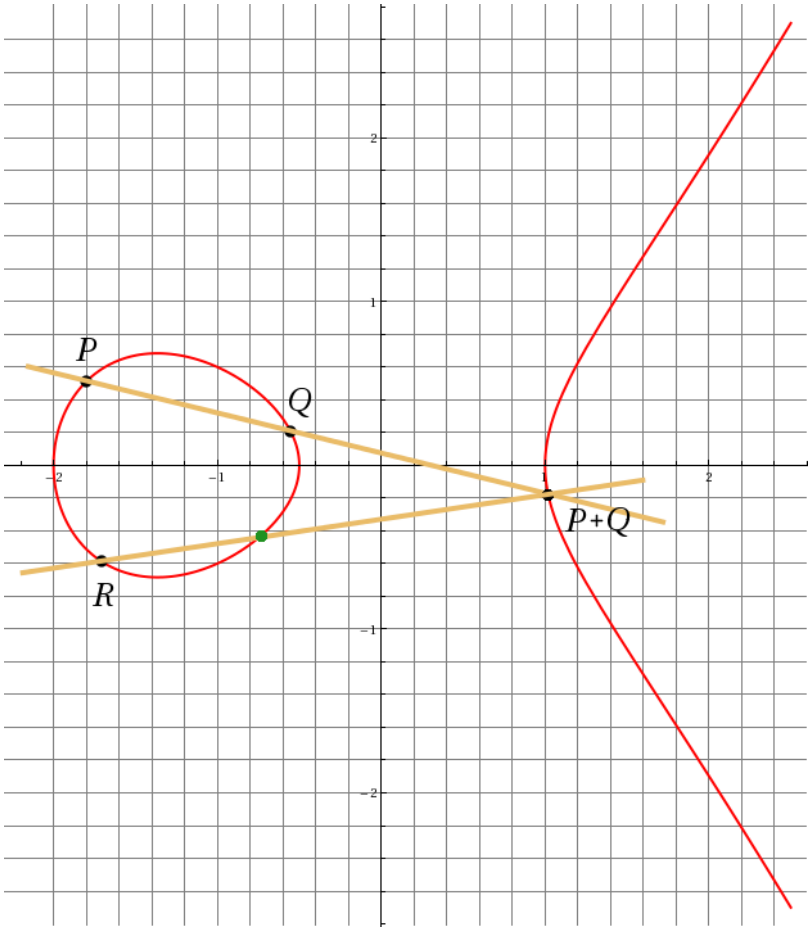
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



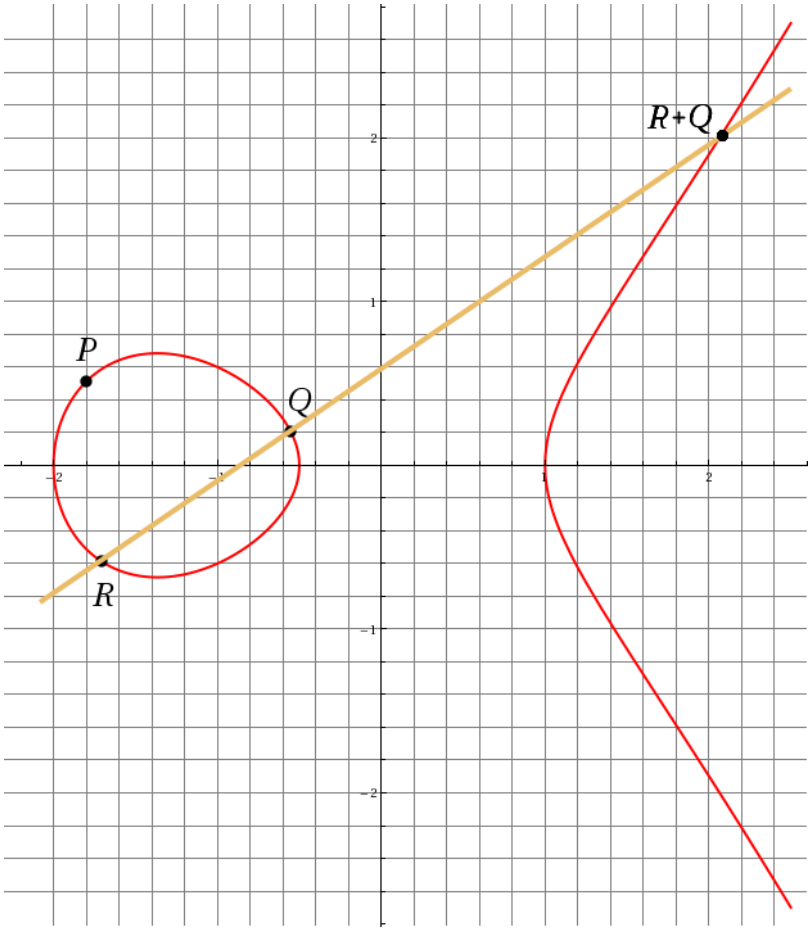
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



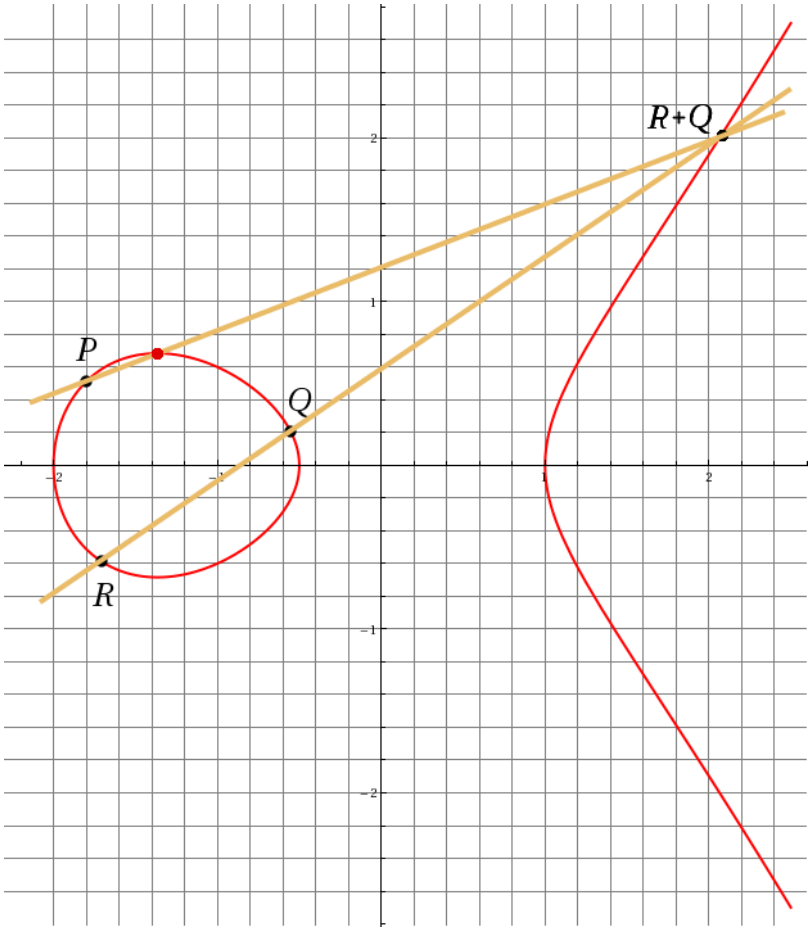
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



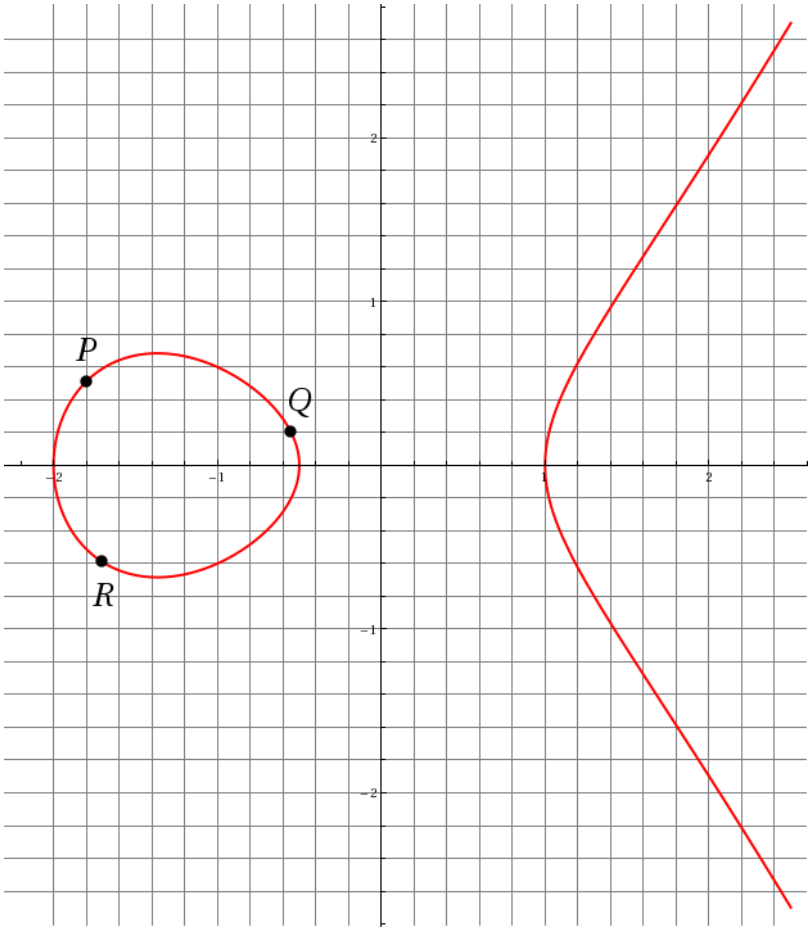
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



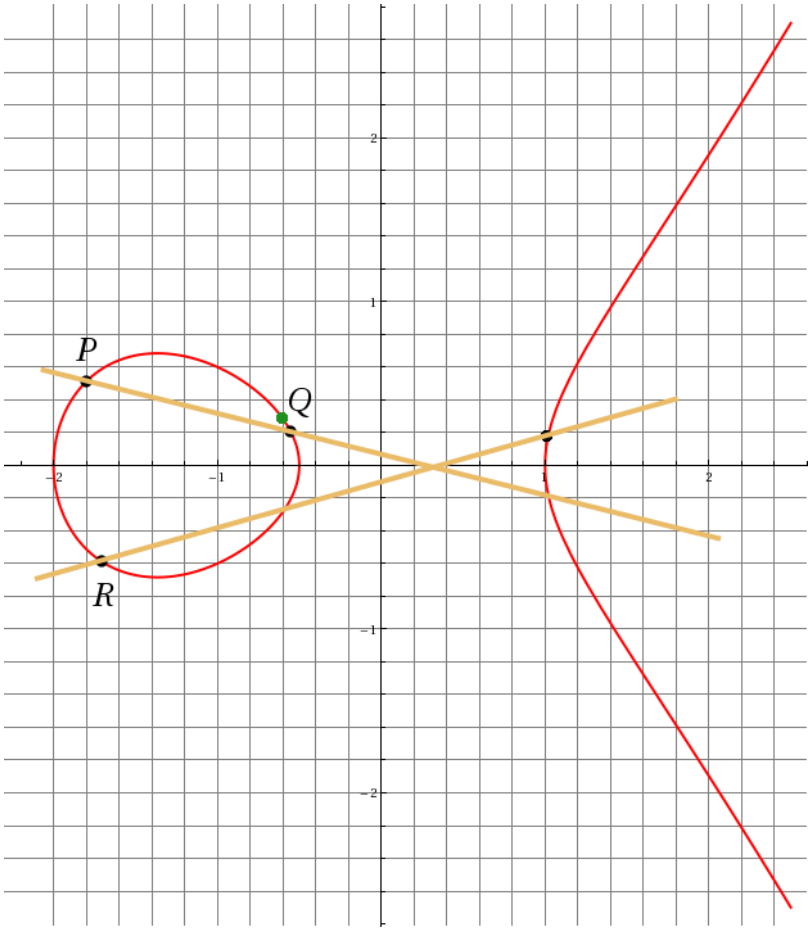
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



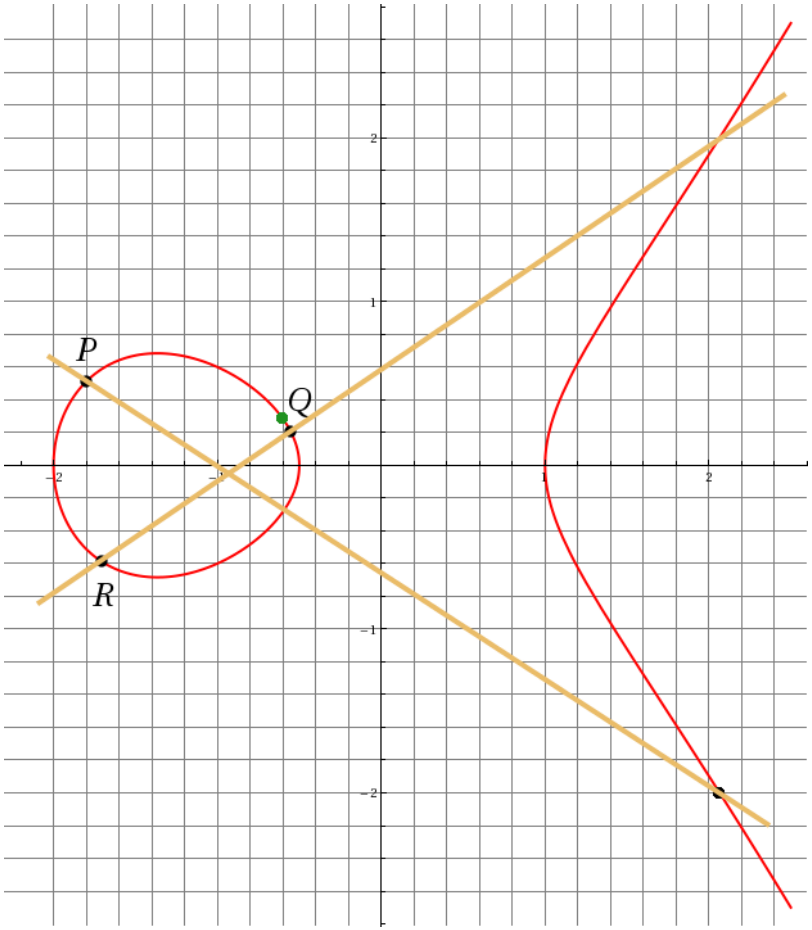
- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?



- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Zakaj prezrcalimo?

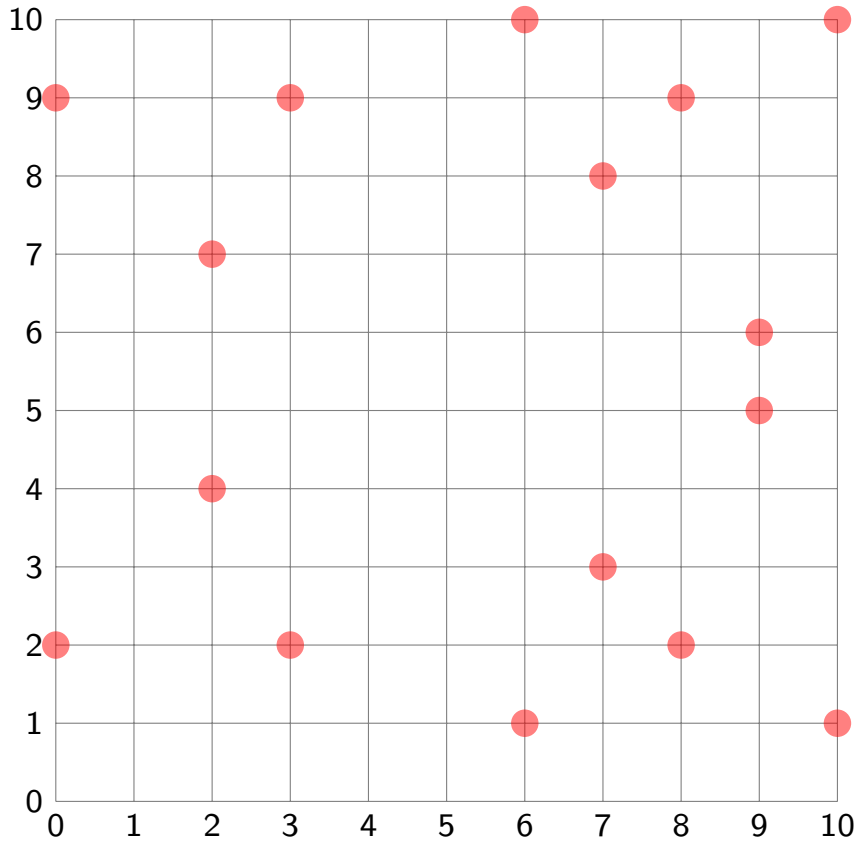


- Kratek račun pokaže, da je $(P + Q) + R = P + (Q + R)$
- Če ne prezrcalimo, to ne velja!

Aritmetika na eliptični krivulji

- Točke lahko seštevamo in računamo njihove večkratnike
- Za šifriranje izberemo točko P in neko naključno število a
- Javni ključ je (E, P, aP)
- Zasebni ključ je a
- Iz aP in P je zelo težko dobiti a
- V praksi gledamo krivulje nad *končnimi obsegi*

Večkratniki točke na eliptični krivulji

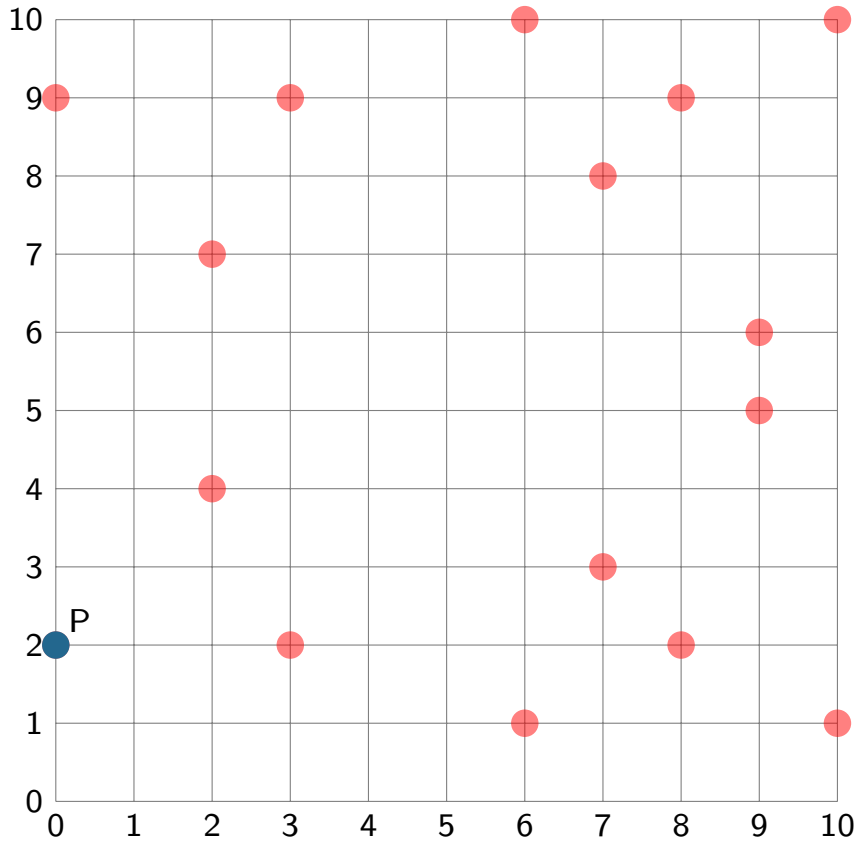


Levo so prikazane vse točke na eliptični krivulji

$$y^2 = x^3 + 2x + 4$$

nad $\mathbb{Z}_{11}$. Dobimo jih tako, da za vse možne vrednosti x preverimo, kdaj je desna stran kvadrat v $\mathbb{Z}_{11}$.

Večkratniki točke na eliptični krivulji

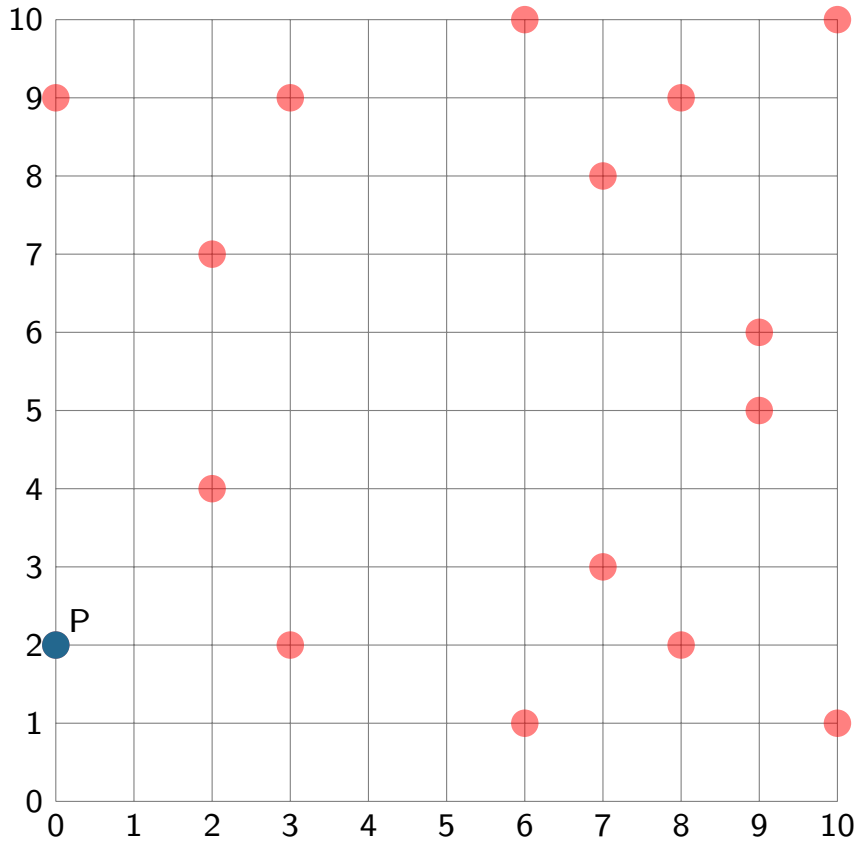


Izberimo neko točko, npr. za $x = 0$. Potem je

$$x^3 + 2x + 4 = 4,$$

zato $y = \pm 2$. Naj bo $P = (0, 2)$. Poglejmo njene večkratnike.

Večkratniki točke na eliptični krivulji



Za $2P = P + P$ izračunamo

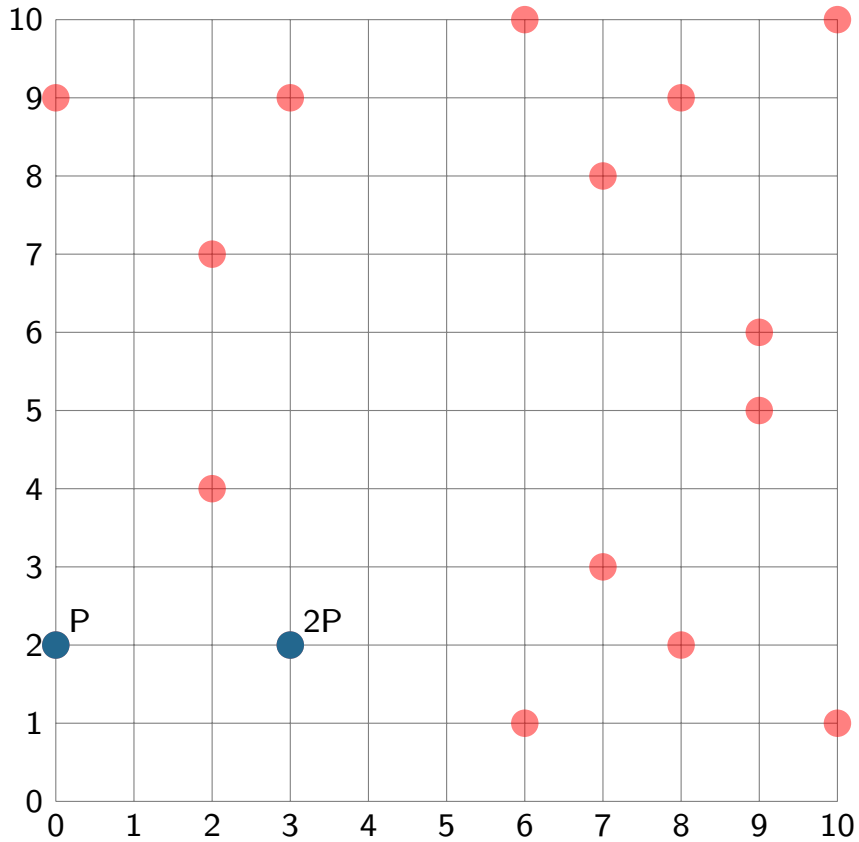
$$\lambda = \frac{3x^2 + a}{2y} = \frac{2}{4} = 6$$

in

$$x_3 = \lambda^2 - 2x = 3,$$
$$y_3 = \lambda(x - x_3) - y = 2,$$

torej je $2P = (3, 2)$.

Večkratniki točke na eliptični krivulji



Za $2P = P + P$ izračunamo

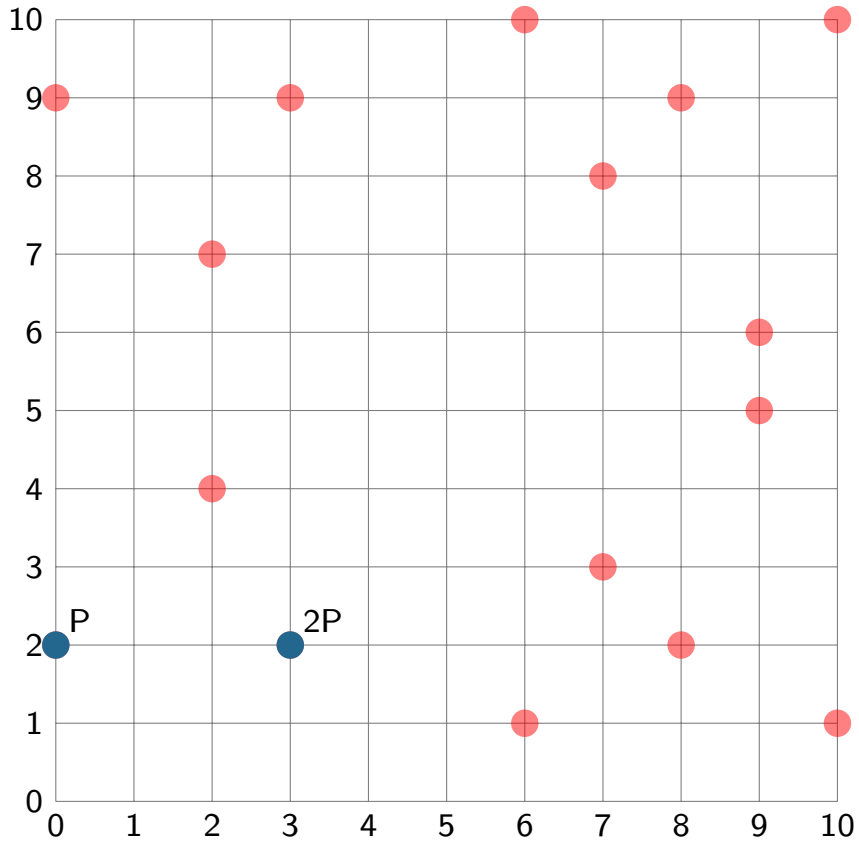
$$\lambda = \frac{3x^2 + a}{2y} = \frac{2}{4} = 6$$

in

$$x_3 = \lambda^2 - 2x = 3,$$
$$y_3 = \lambda(x - x_3) - y = 2,$$

torej je $2P = (3, 2)$.

Večkratniki točke na eliptični krivulji



Nadaljujemo s $3P = 2P + P$.
Tokrat je

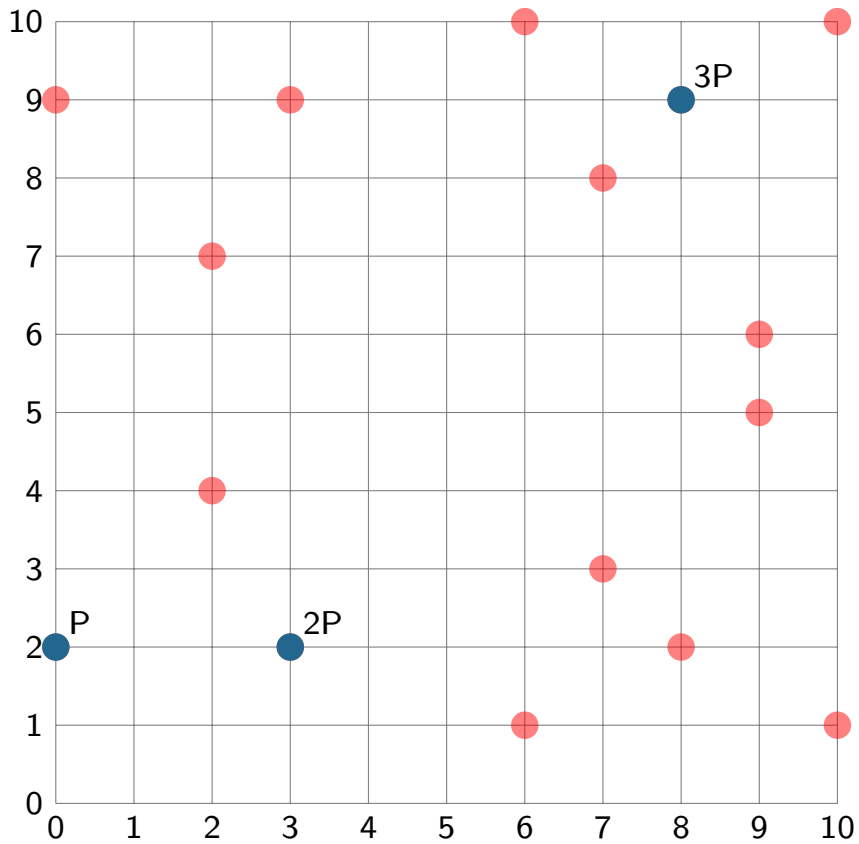
$$\lambda = \frac{2-2}{3-0} = 0$$

in

$$x_3 = \lambda^2 - 3 - 0 = 8,$$
$$y_3 = \lambda(3 - x_3) - 2 = 9,$$

torej je $3P = (8, 9)$.

Večkratniki točke na eliptični krivulji



Nadaljujemo s $3P = 2P + P$.
Tokrat je

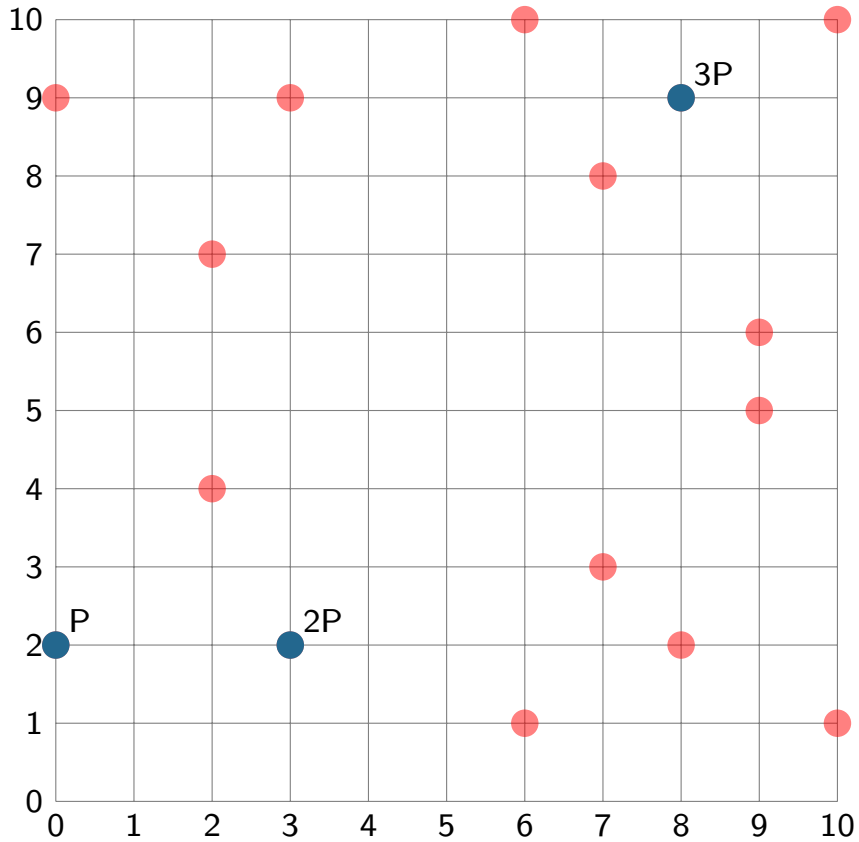
$$\lambda = \frac{2-2}{3-0} = 0$$

in

$$x_3 = \lambda^2 - 3 - 0 = 8,$$
$$y_3 = \lambda(3 - x_3) - 2 = 9,$$

torej je $3P = (8, 9)$.

Večkratniki točke na eliptični krivulji



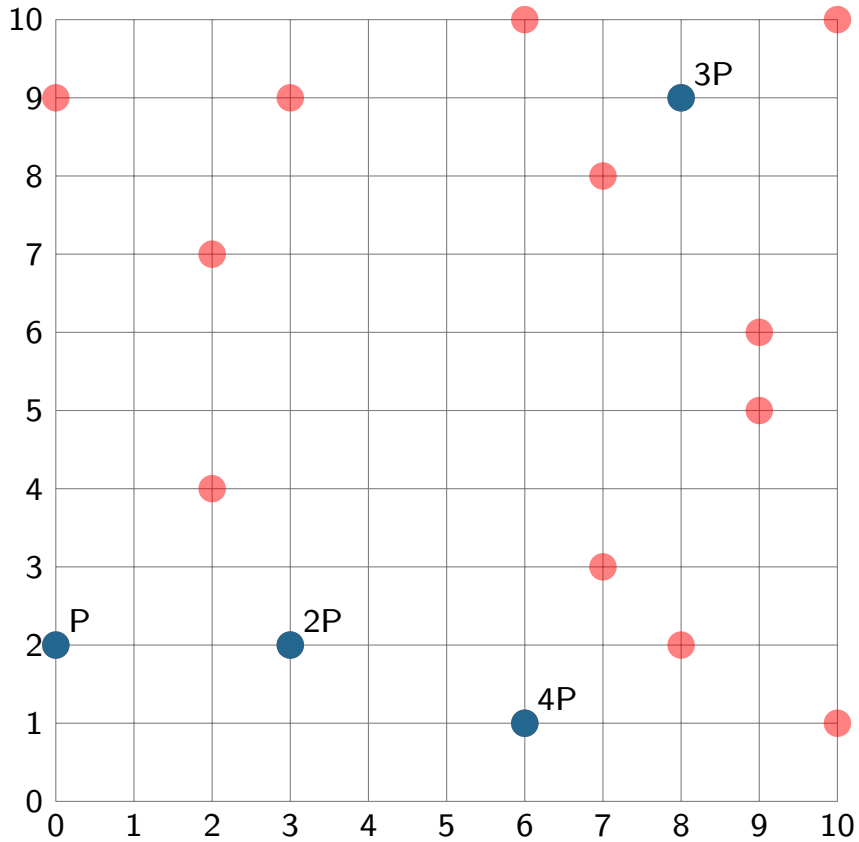
Pri $4P = 2P + 2P = 3P + P$ imamo dve možnosti. Pri prvem načinu je

$$\lambda = \frac{3 \cdot 3^2 + 2}{2 \cdot 2} = \frac{7}{4} = 10,$$

$$x_3 = \lambda^2 - 2 \cdot 3 = 6,$$
$$y_3 = \lambda(3 - x_3) - 2 = 1,$$

torej je $4P = (6, 1)$.

Večkratniki točke na eliptični krivulji



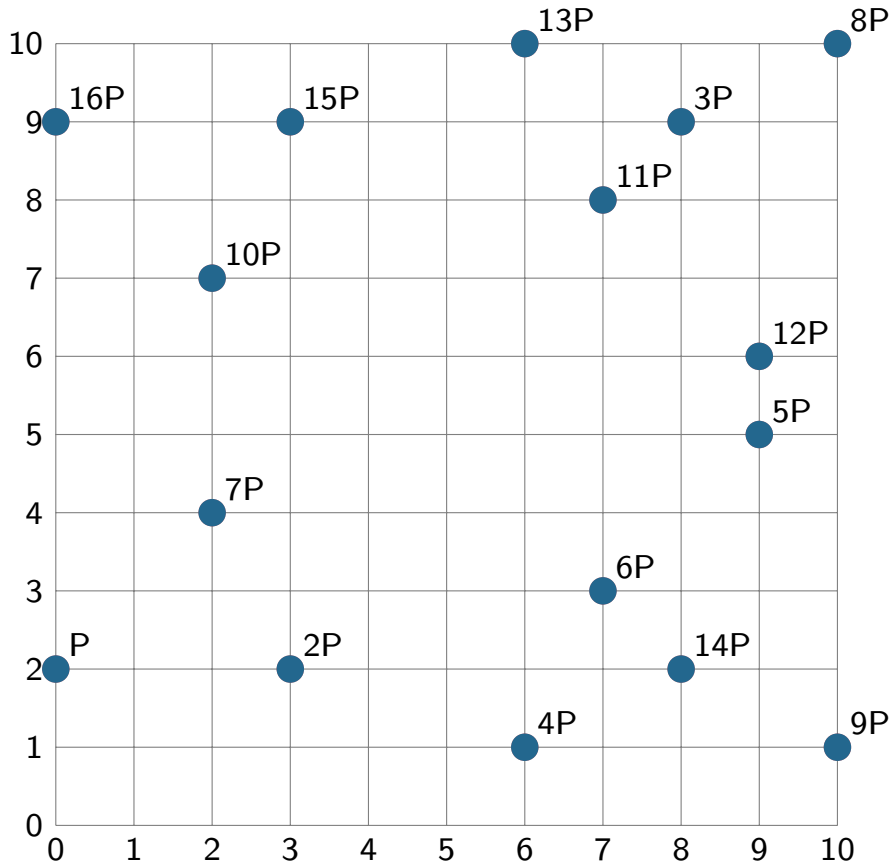
Pri drugem načinu je

$$\lambda = \frac{9-2}{8-0} = \frac{7}{8} = 5,$$

$$x_3 = \lambda^2 - 8 - 0 = 6,$$
$$y_3 = \lambda(8 - x_3) - 9 = 1,$$

in kot prej $4P = (6, 1)$.

Večkratniki točke na eliptični krivulji



Nadaljujemo še z ostalimi točkami.
Za $16P$ dobimo $(0, 9)$, kar je ravno $-P$, torej je $17P = \mathcal{O}$ točka v neskončnosti.

Kako izračunati kP

- Za majhne k lahko seštejemo $P + P + \cdots + P$
- Za velike k to ni praktično
- Pomagamo si z dvojiškim zapisom:

$$k = 2^n + k_{n-1}2^{n-1} + \cdots k_2 2^2 + k_1 2 + k_0,$$

$k_i = 0$ ali 1. Potem je

$$kP = 2^n P + k_{n-1}2^{n-1}P \cdots + k_1 2P + k_0 P$$

- Najprej s podvajanjem izračunamo $2^\ell P$, nato samo seštejemo prave

Primer

- Izračunajmo $23P$!
- Najprej zapišemo

$$23 = 16 + 4 + 2 + 1$$

- Nato izračunamo $2P$, $4P$, $8P$, $16P$
- Na koncu seštejemo $16P + 4P + 2P + P$
- Skupaj torej $4 + 3 = 7$ operacij

Kako šifriramo z eliptičnimi krivuljami

- Imamo krivuljo E in točko P na njej
- Izberemo si naključno število a, $A = aP$
- Javni ključ je (E, P, A), zasebni je a
- Za šifriranje X izberemo naključen k in izračunamo par $(kP, X + kA)$
- Dešifriranje para (Y_1, Y_2) opravimo kot $Y_2 - aY_1$

Primer

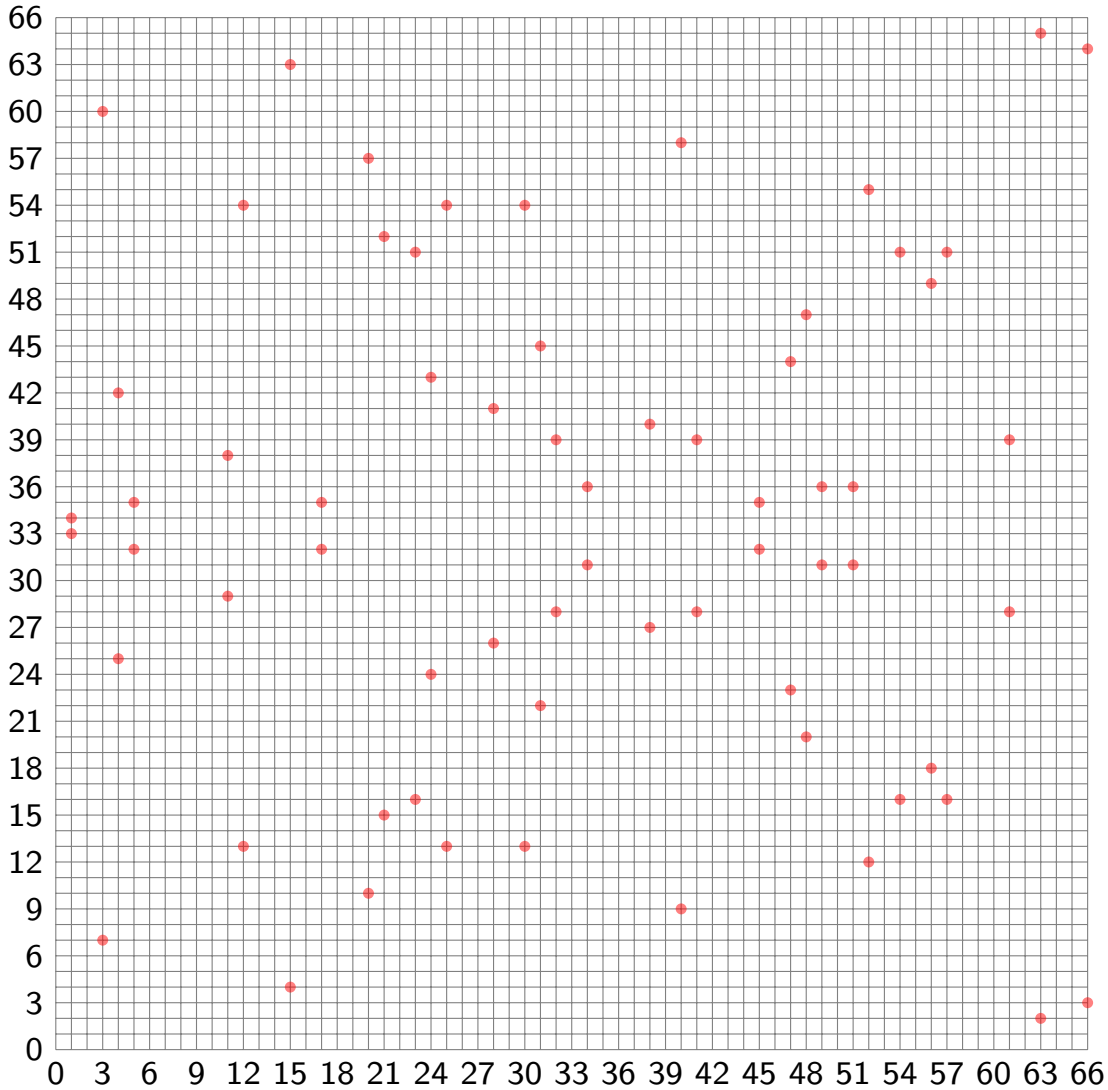
Vzemimo eliptično krivuljo $y^2 = x^3 + 2x + 4$ nad $\mathbb{Z}_{11}$ in $P = (0, 2)$.

- Anita si za zasebni ključ izbere $a = 5$. Njen javni ključ je $A = aP = 5P = (9, 5)$
- Če želi Bojan Aniti poslati $X = (2, 4)$, najprej izbere nek naključen k, npr. $k = 8$.
- Bojan izračuna par $(8P, X + 8A)$, torej $((10, 10), (2, 4) + (7, 3)) = ((10, 10), (6, 10))$ in ga pošlje Aniti
- Anita za dešifriranje izračuna $(6, 10) - 5(10, 10) = (2, 4)$

Kako to uporabiti za šifriranje?

- Kombinacija simetrične in asimetrične kriptografije
- S pomočjo javnih ključev si izmenjamo ključ za simetrično šifro
- Npr. v točki $X = (x, y)$ x predstavlja stran v neki knjigi, y pa zaporedno besedo
- Dobljeno besedo uporabimo v Vigenerjevi šifri

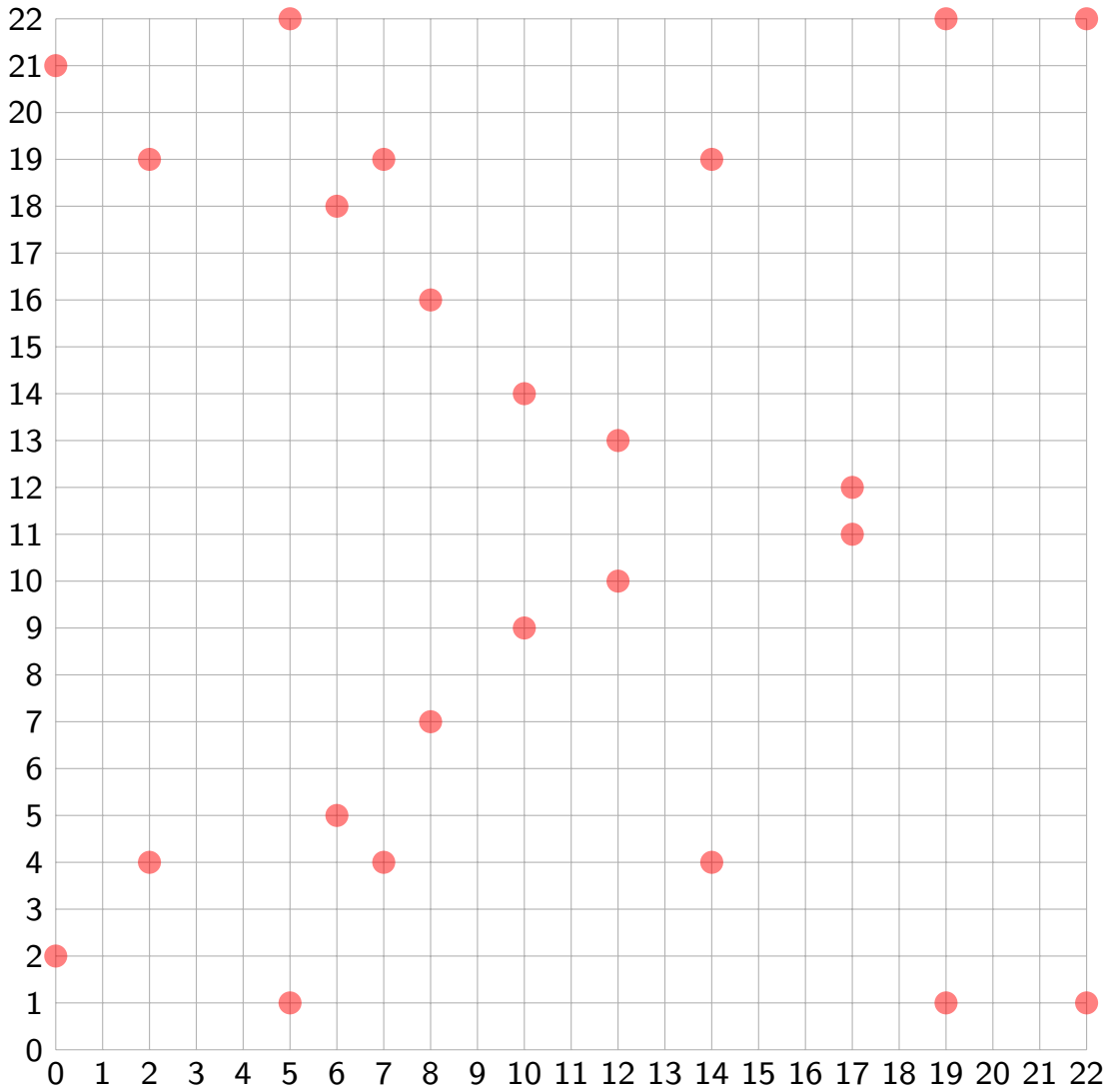
Praktičen primer



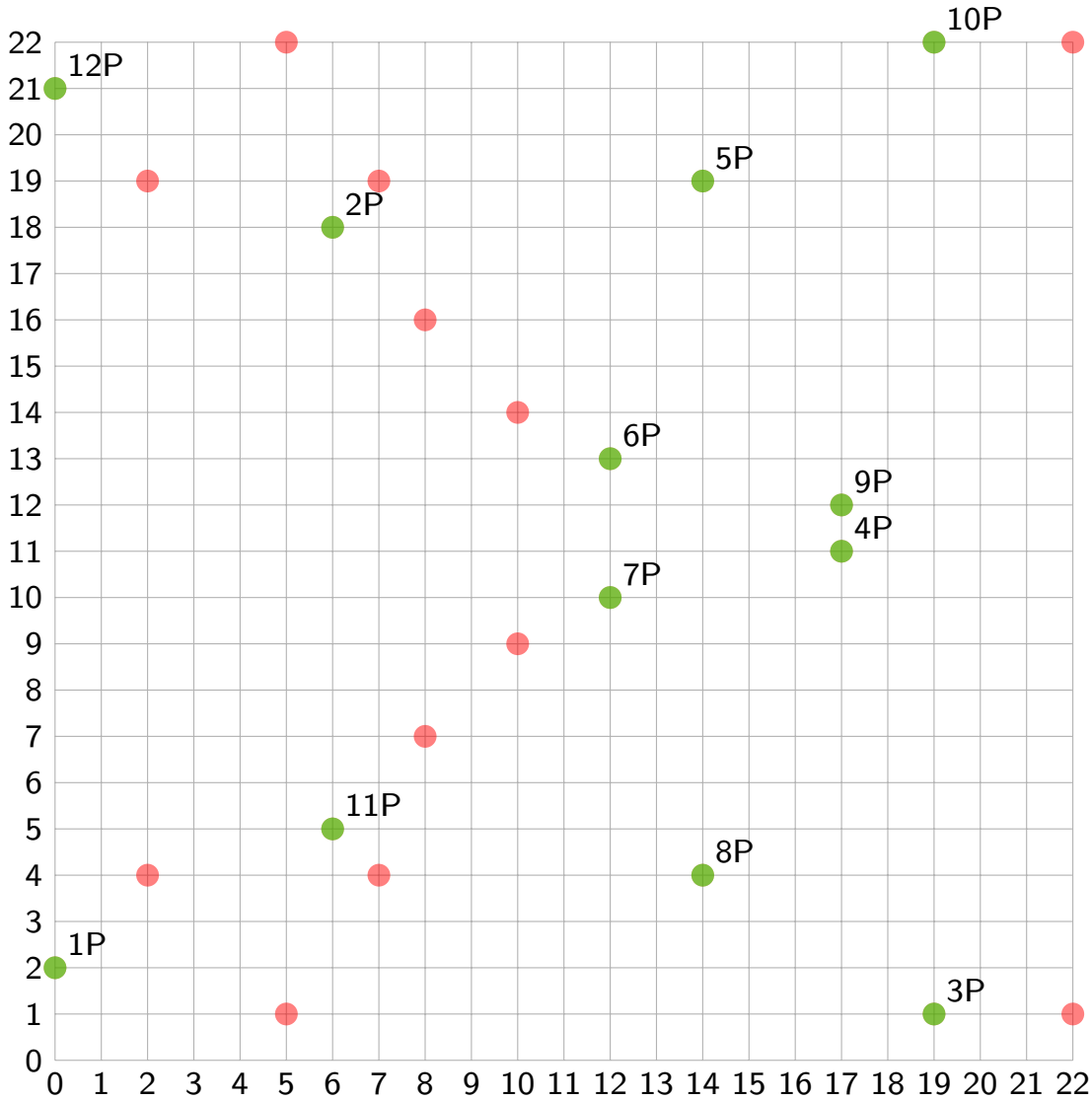
Na sliki na levi so točke na eliptični krivulji

$$y^2 = x^3 + 3x + 13$$

nad $\mathbb{Z}_{67}$.
Točk (skupaj z $\mathcal{O}$) je 67.



Na levi je primer krivulje, kjer večkratniki izbrane točke ne pokrijejo celotne krivulje.



Na levi je primer krivulje, kjer večkratniki izbrane točke ne pokrijejo celotne krivulje.

Vprašanja