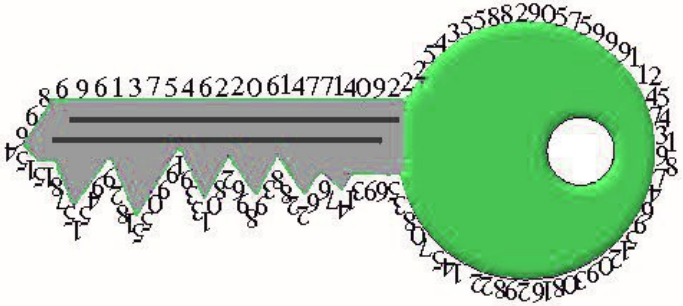
Zgodovina kriptografije in Matematika šifriranja

Jernej Tonejc

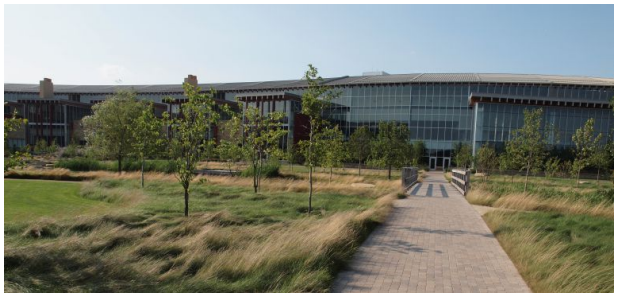


MARS

18. avgust 2012

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
- ∼2 leti delal za EPIC

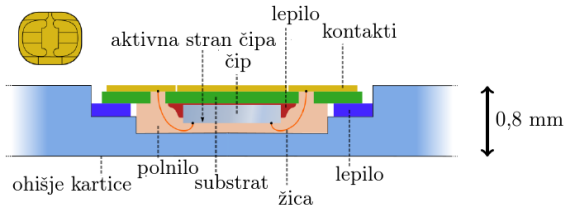


O meni

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



  - Varno vložišče
  - Pametne kartice za MORS



Načrt

- Kratka zgodovina kriptografije (danes)
- Matematične osnove (nedelja)
- RSA in praštevila (ponedeljek)
- Napadi na RSA (torek)

Načrt za matematične osnove

- Modularna aritmetika in deljivost
- $\mathbb{Z}_p$, $\mathbb{Z}_n^*$, Fermatov in Eulerjev izrek
- Zahtevnost potenciranja
- Kitajski izrek o ostankih (KIO)

Načrt za RSA

- Ideja RSA in problem faktorizacije
- Iskanje praštevil
- Šifriranje, dešifriranje, podpisovanje
- Pohitritev s KIO

Načrt za napade na RSA

- Neprimerna izbira praštevil p in q
- Podpisovanje naključnih sporočil
- Napadi s stranskim kanalom
- Napad na pohitritev s KIO

Kratka zgodovina kriptografije

- **Osnove kriptografije**
- Klasični tajnopisi
- Simetrična kriptografija
- Kriptografija z javnimi ključi
- Kriptoanaliza

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

Ana

Glavni igralci

Ana

Blaž

Glavni igralci

Ana

komunicirata

Blaž

Glavni igralci

Ana

Blaž

komunicirata

prisluškuje

Oskar

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.

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.

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.

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.

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

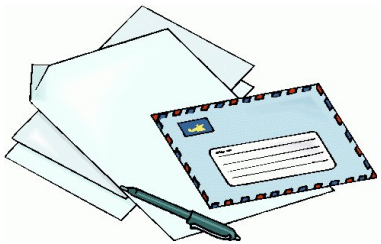
Kakšna zagotovila varnosti imamo? Na kakšen način?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura

Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Na kakšen način?

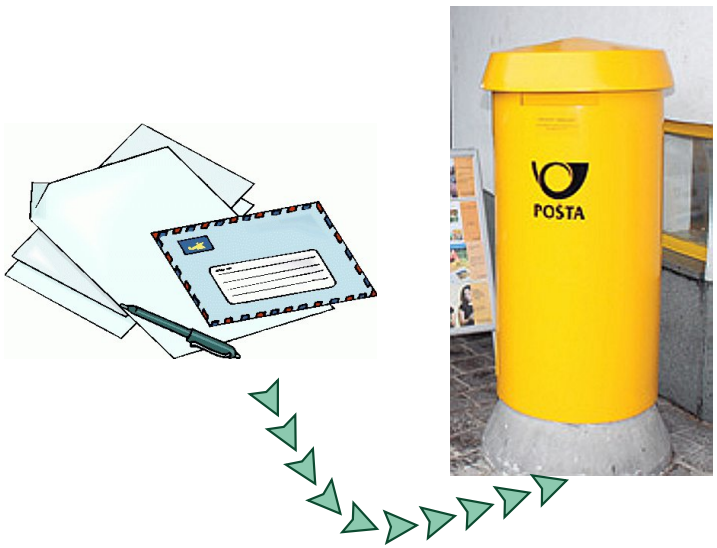
- Fizična varnost
- Zakonodaja
- Poštna infrastruktura



Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Na kakšen način?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura



Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Na kakšen način?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura

Primer: pošiljanje običajnih dokumentov po pošti

Kakšna zagotovila varnosti imamo? Na kakšen način?

- Fizična varnost
- Zakonodaja
- Poštna infrastruktura

Primer: elektronski podatki

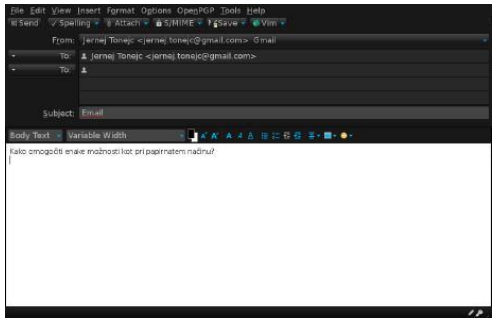
Kako omogočiti enake možnosti kot pri papirnatem načinu?

- ⊕ Enostavno in poceni hranjenje
- ⊕ Hitro in enostavno prenašanje
- ⊖ Enostavno kopiranje
- ⊖ Prenosi niso (nujno) varni

Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirnatem načinu?

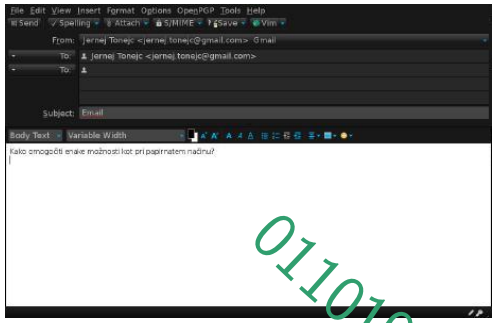
- $\oplus$ Enostavno in poceni hranjenje
- $\oplus$ Hitro in enostavno prenašanje
- $\ominus$ Enostavno kopiranje
- $\ominus$ Prenosi niso (nujno) varni

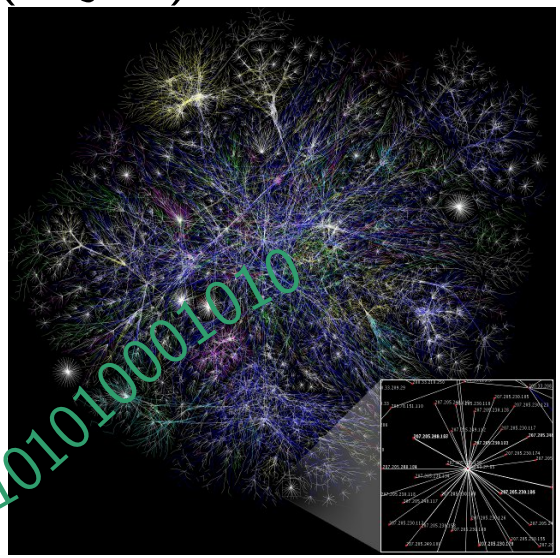


Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirnatem načinu?

- ⊕ Enostavno in poceni hranjenje
- ⊕ Hitro in enostavno prenašanje
- ⊖ Enostavno kopiranje
- ⊖ Prenosi niso (nujno) varni

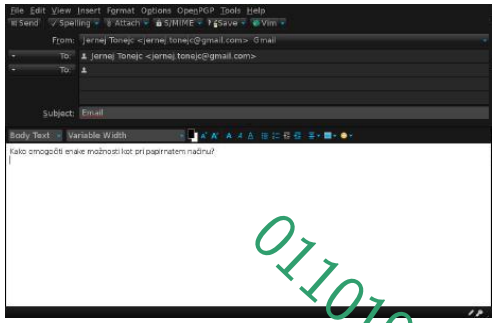


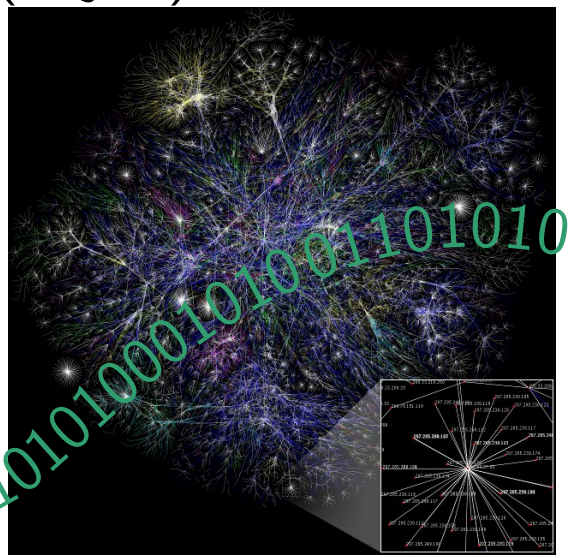


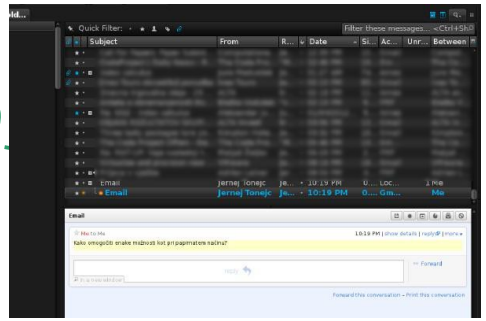
Primer: elektronski podatki

Kako omogočiti enake možnosti kot pri papirnatem načinu?

- ⊕ Enostavno in poceni hranjenje
- ⊕ Hitro in enostavno prenašanje
- ⊖ Enostavno kopiranje
- ⊖ Prenosi niso (nujno) varni







Kratka zgodovina kriptografije

- Osnove kriptografije
- **Klasični tajnopisi**
- Simetrična kriptografija
- Kriptografija z javnimi ključi
- Kriptoanaliza

Začetki

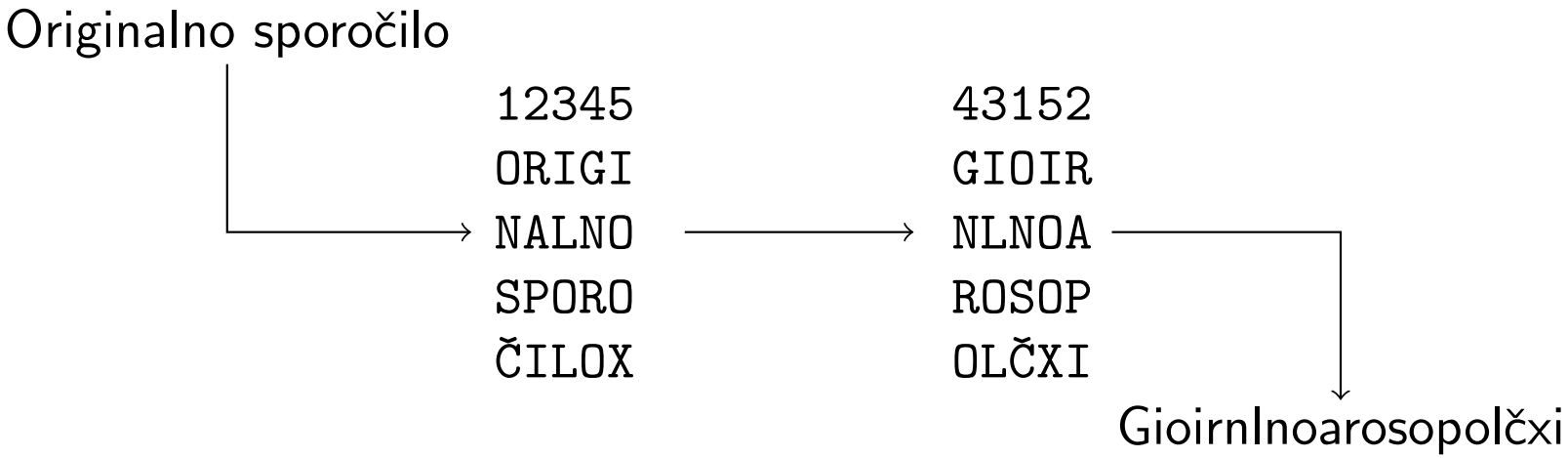
- Najstarejši znani tajnopisi v Egiptu (∼ 2500 pr.n.št.)

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

Transpozicijska šifra

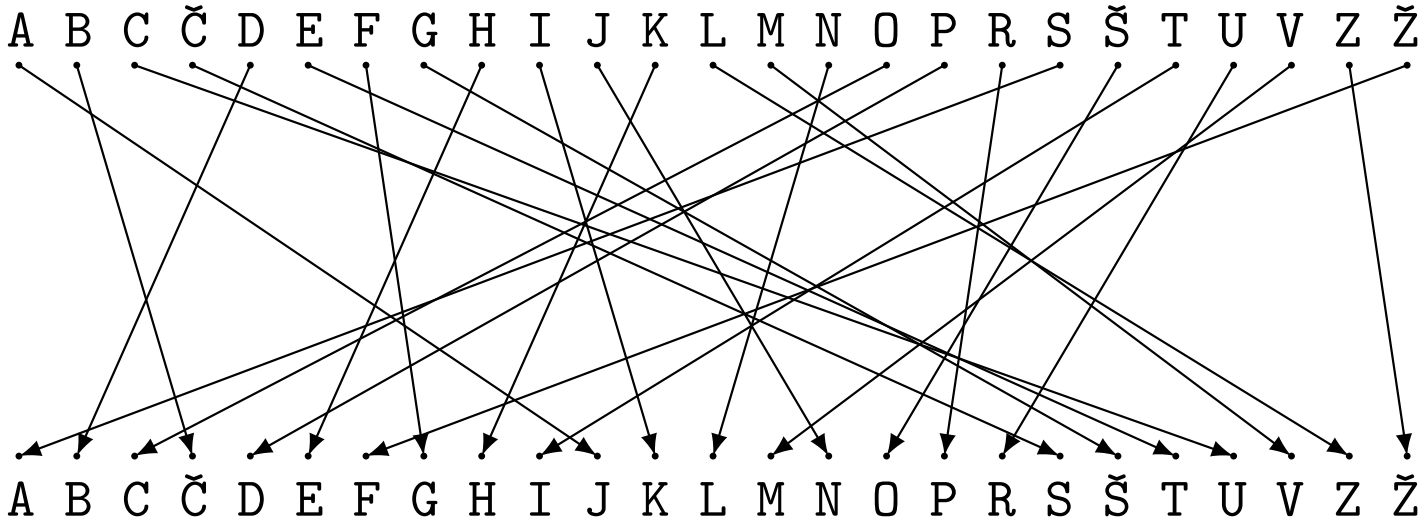
- Črke originalnega sporočila ostanejo nespremenjene, njihova mesta pa so pomešana
- Zlahka prepoznamo, če izračunamo gostoto samoglasnikov ($\sim 41\%$ v slovenščini)
- Primer: Skytale

Primer: permutacija stolpcev



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



Substitucijska šifra, nad.

- Vseh permutacij 25 črk je $25! \approx 1{,}55 \times 10^{25}$
- Splošno permutacijo si je težko zapomniti, zato uporabimo ključno črko in besedo
- Primer: Črka J in beseda ZELOHUDOGESLO

  ABCČDEFGHIJKLMNOPRSŠTUVZŽ

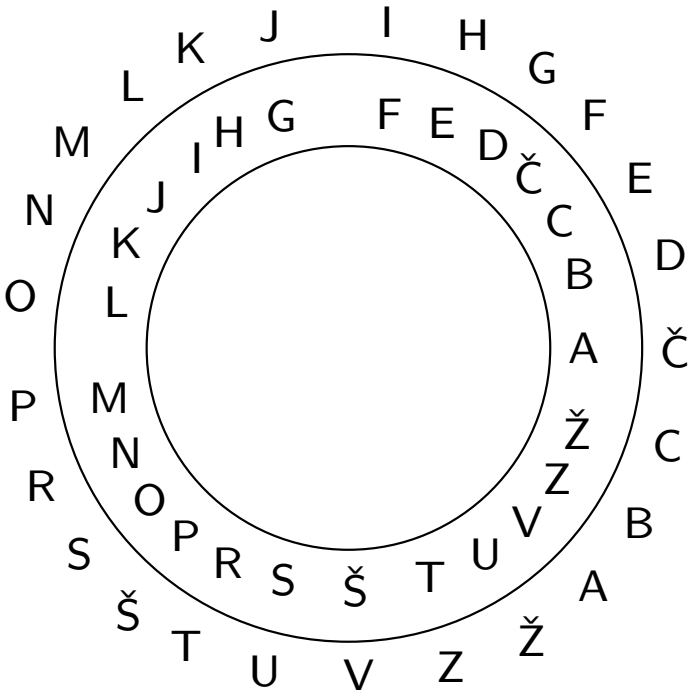
  ZELOHUDGS

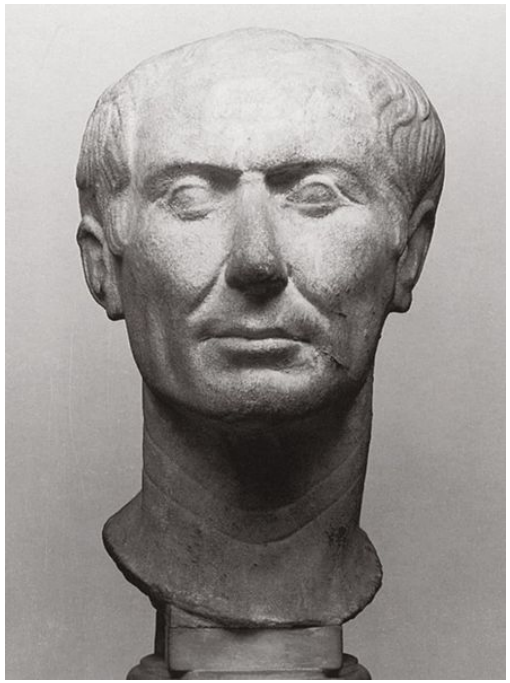
  JKMNPRŠTVŽZELOHUDGSABCČFI

  A→J, B→K, C→M, Č→N, ...
- Problem: zaporedne črke se šifrirajo v (skoraj) zaporedne

Pomična šifra

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





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

Modularna aritmetika

- Primer: ura. Ko pridemo do 12 (24), nadaljujemo
- Ostanek pri deljenju z **modulom** m
- Operacije kot običajno. Če presežemo m, popravimo.
- Primer:

$$(3+6) \bmod 7 = 9 \bmod 7 = (7+2) \bmod 7 = 0+2 = 2$$
$$(3*6) \bmod 7 = 18 \bmod 7 = (14+4) \bmod 7 = 0+4 = 4$$

- Velja $m \bmod m = 0$.
- Pri Cezarjevi šifri črke A,...,Ž predstavimo s števili od 0 do 24, prištevamo 3 in računamo po modulu 25.

Afina šifra

- Posplošitev pomične šifre
- Za a in b med 0 in 24 izračunamo

$$x \mapsto a * x + b \pmod{25}$$

- Veljati mora $\mathrm{D}(a, 25) = 1$.
- Za $a = 1$ dobimo pomično šifro.
- Možnih ključev: $20 \times 25 = 500$
  (slabi a-ji so $0, 5, 10, 15, 20$)
- Enoabecedna šifra - vsaka črka se zamenja z natanko določeno črko.

Vigenèrjeva šifra (1586)

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

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
  $\Rightarrow$ 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

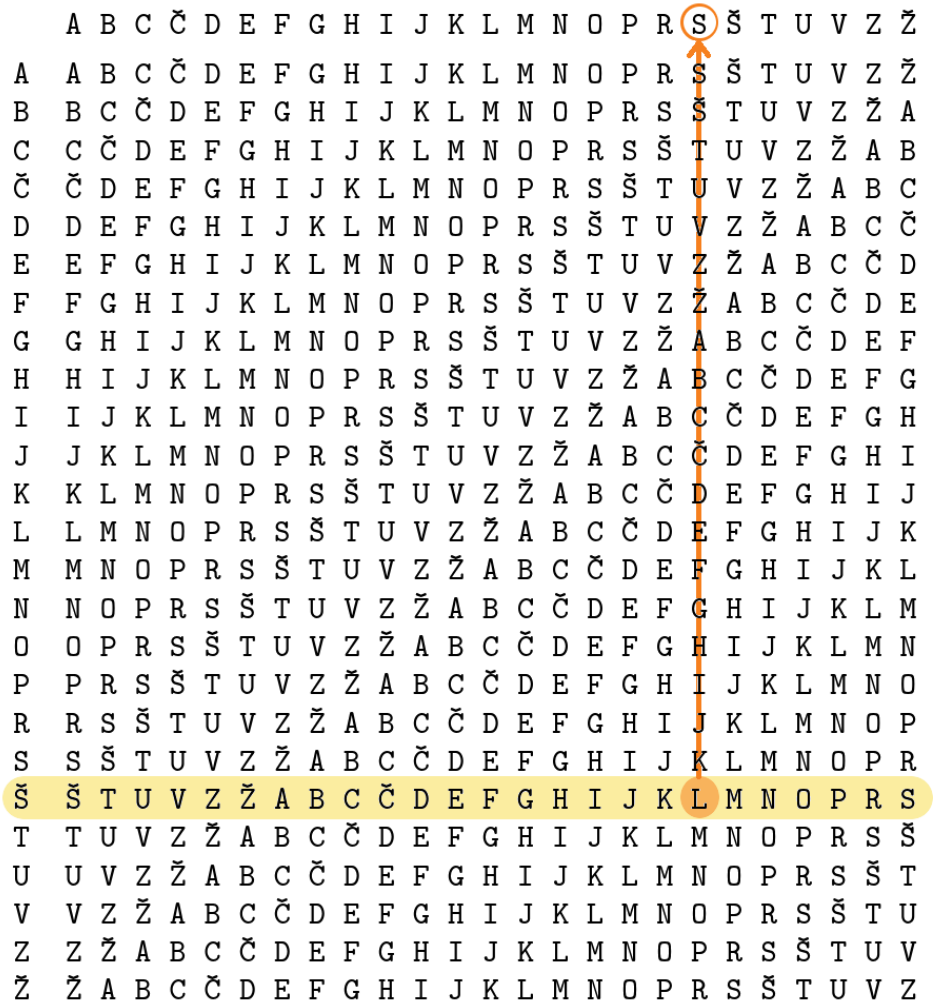
Primer

- 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

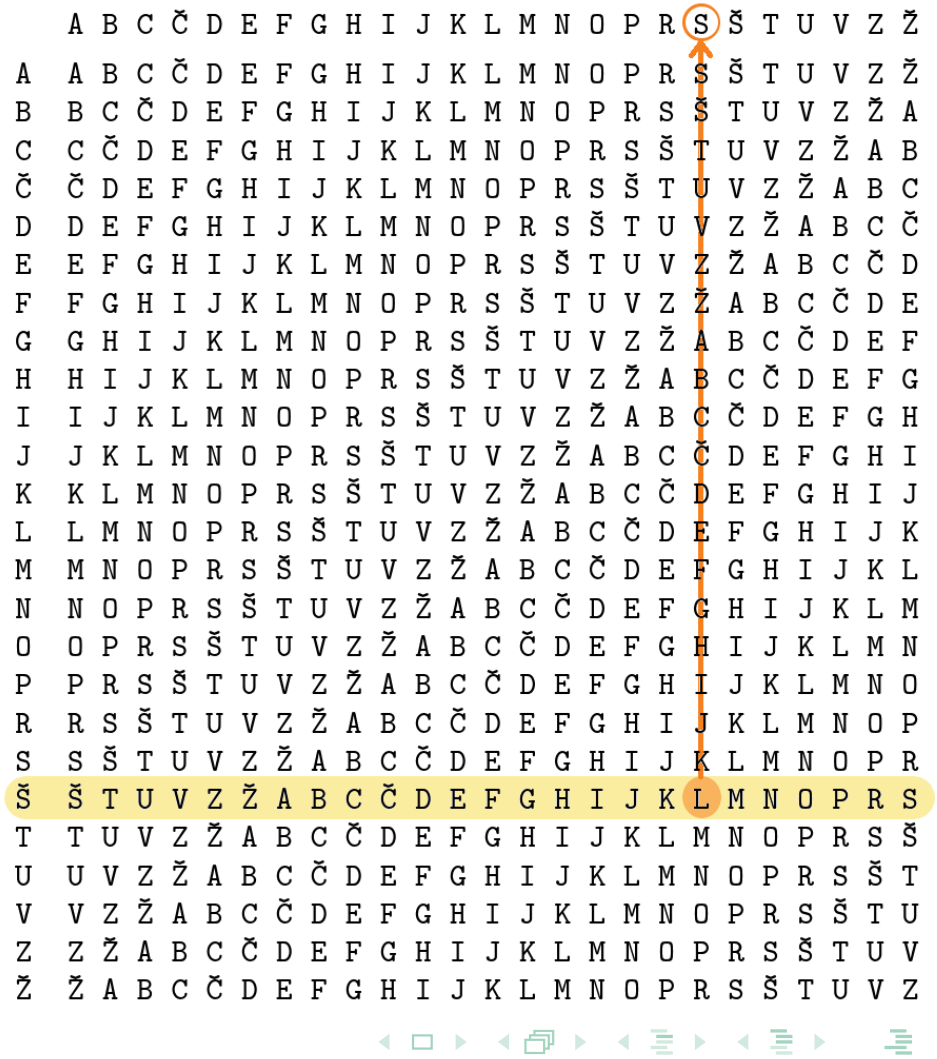
Primer

- 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



Kratka zgodovina kriptografije

- Osnove kriptografije
- Klasično tajnopisje
- **Simetrična kriptografija**
- Kriptografija z javnimi ključi
- Kriptoanaliza

Osnovne lastnosti

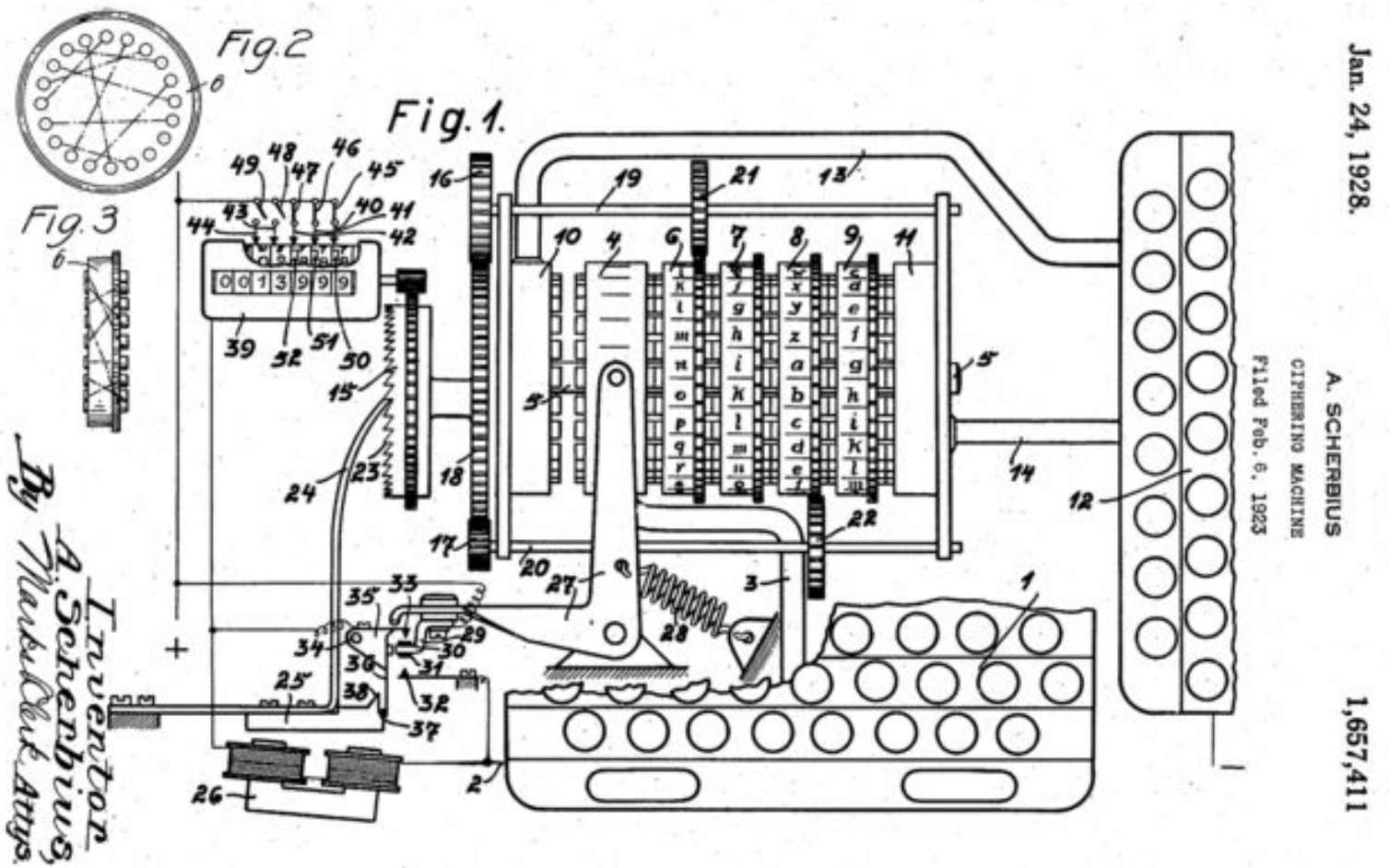
- Najstarejša oblika kriptografije
- Vse do Diffie-Hellmanove objave leta 1976 edina javno znana oblika
- Poznavanje enega ključa omogoča tako šifriranje kot dešifriranje sporočil $\Rightarrow$ simetrija
- V praksi dosega visoke hitrosti (VIA procesor s strojno podporo za AES lahko šifrira več kot 25Gb/s)

Primeri: 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.

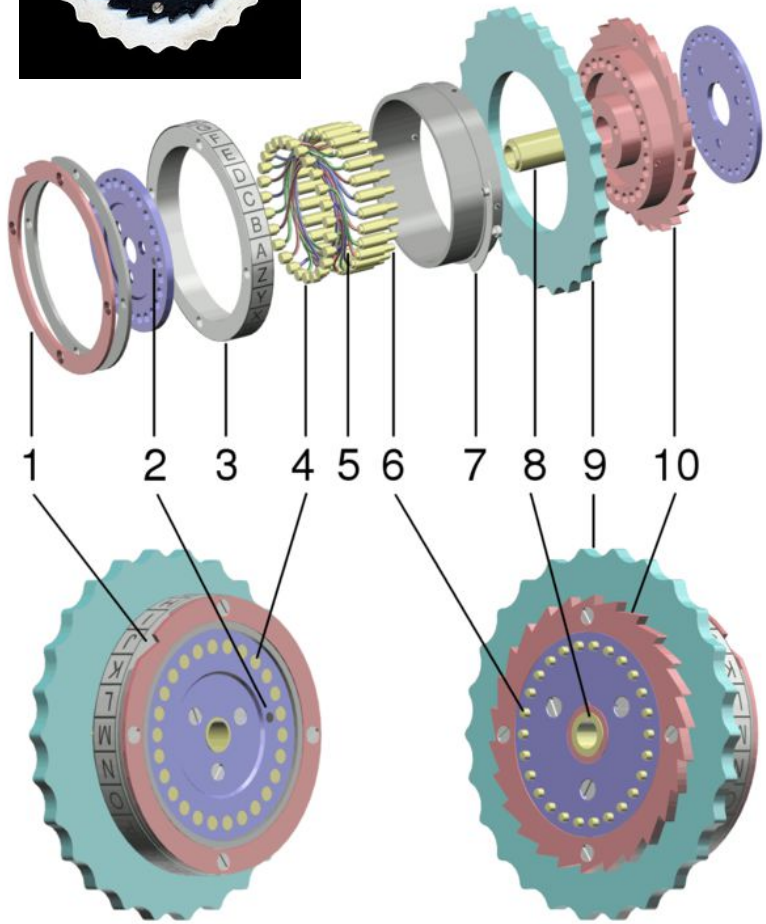
Simulacija na http://enigmaco.de/

Patent za Enigmo

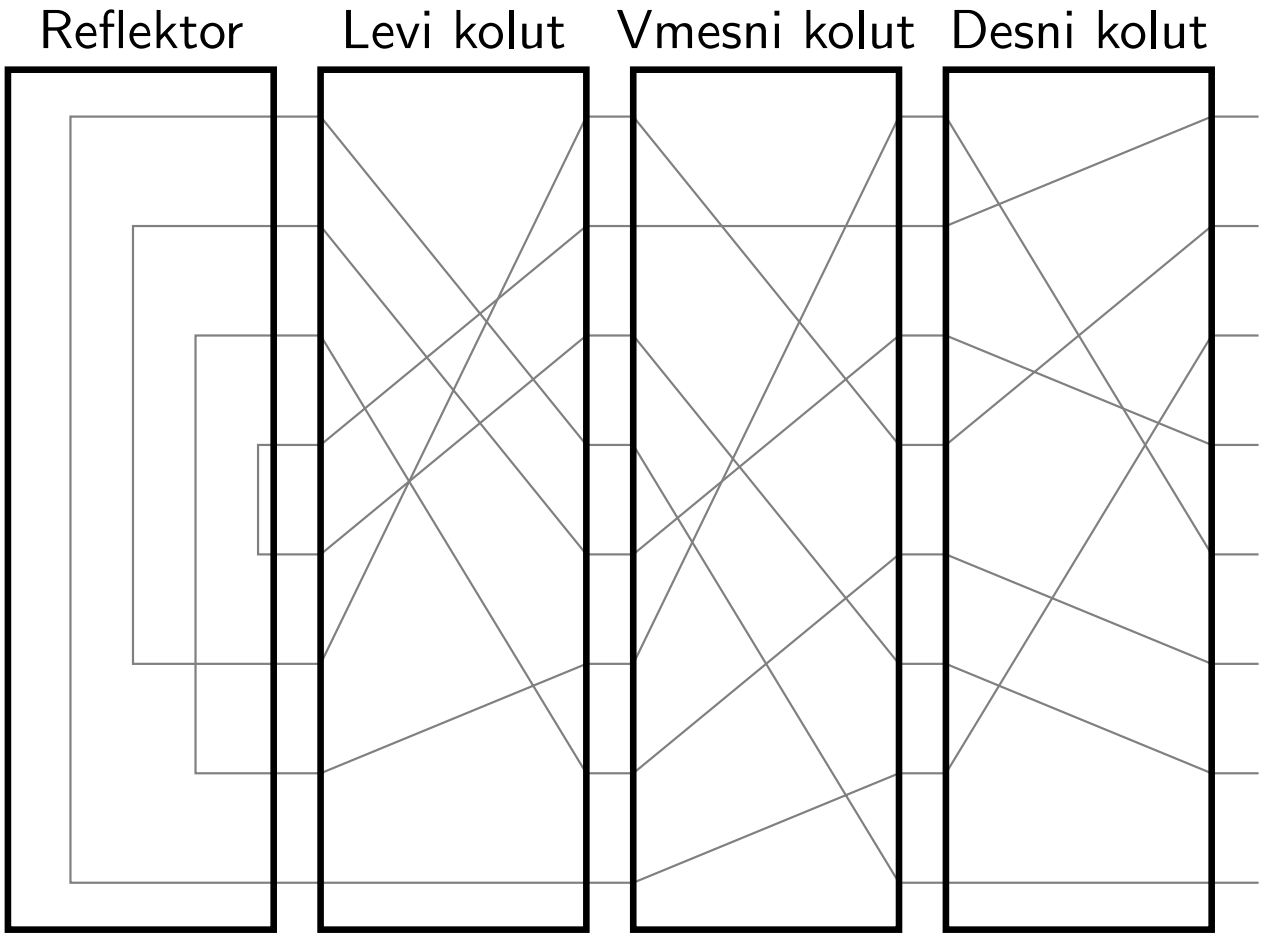


Zgradba kolutov

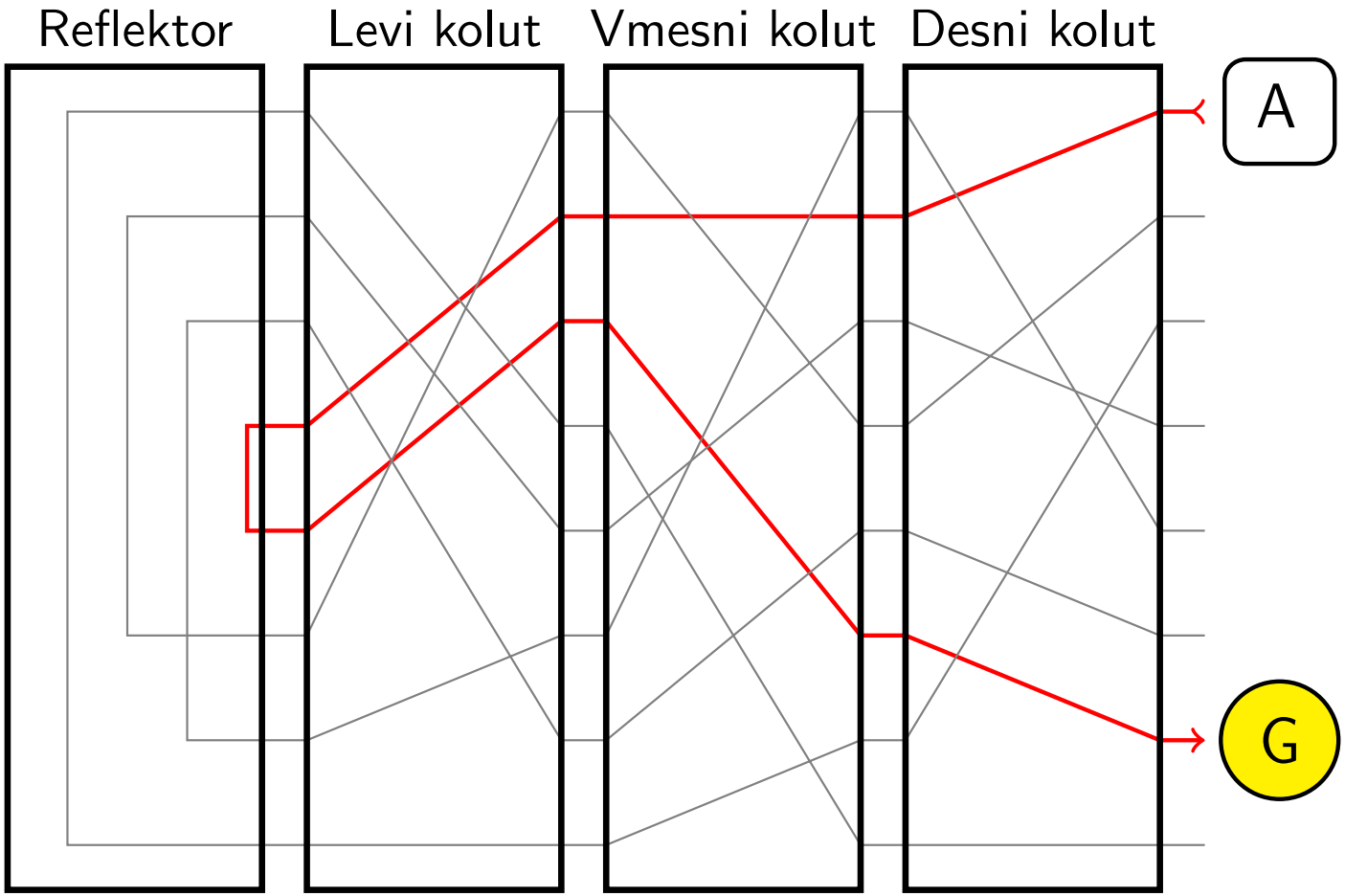
1. Obroč z utorom
2. Oznaka za 'A'
3. Obroč s črkami
4. Plošča s kontakti
5. Povezave
6. Zatiči s kontakti
7. Nastavitveni obroč
8. Os
9. Kolut za ročni pomik
10. Obroč z zarezami



Princip delovanja

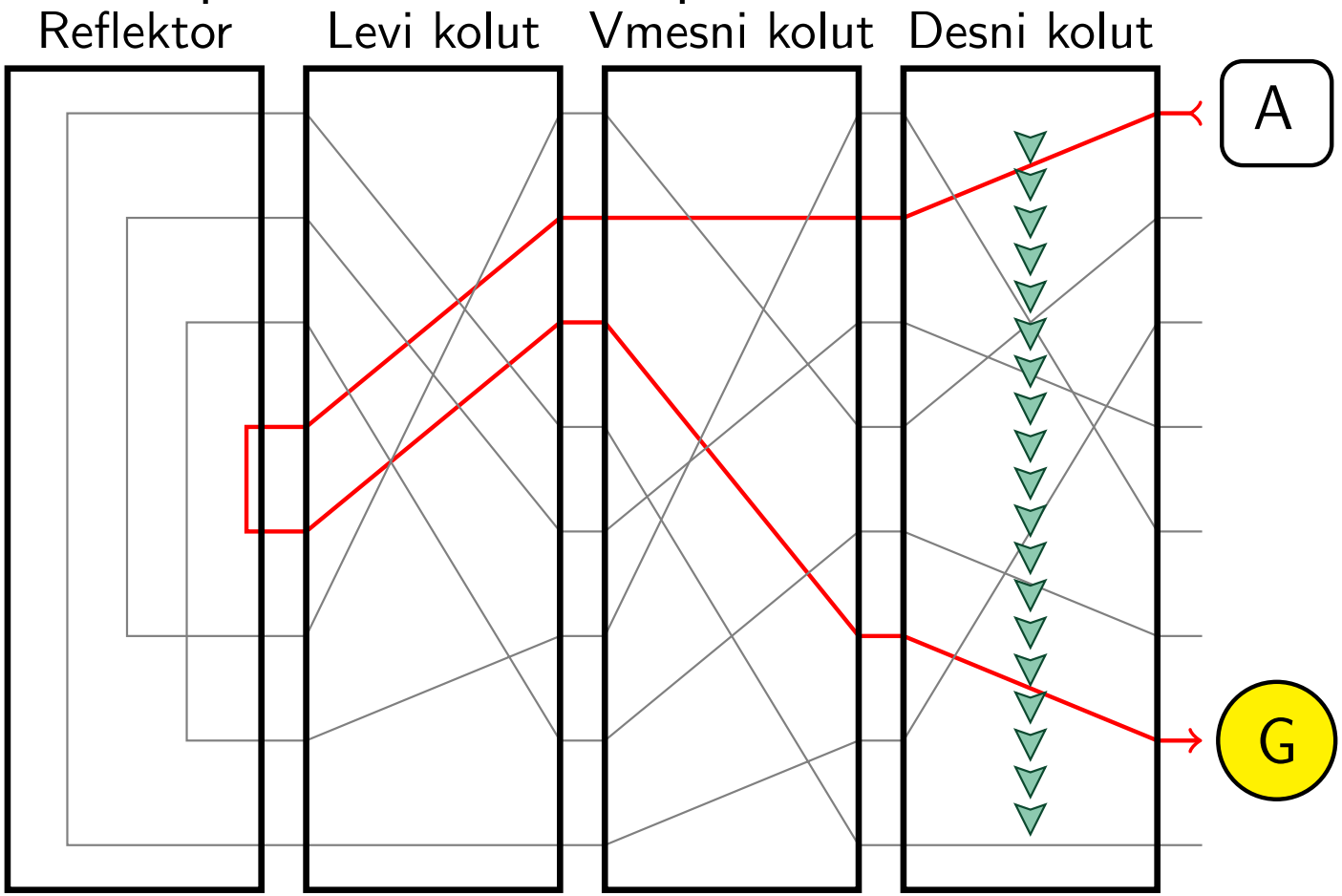


Princip delovanja

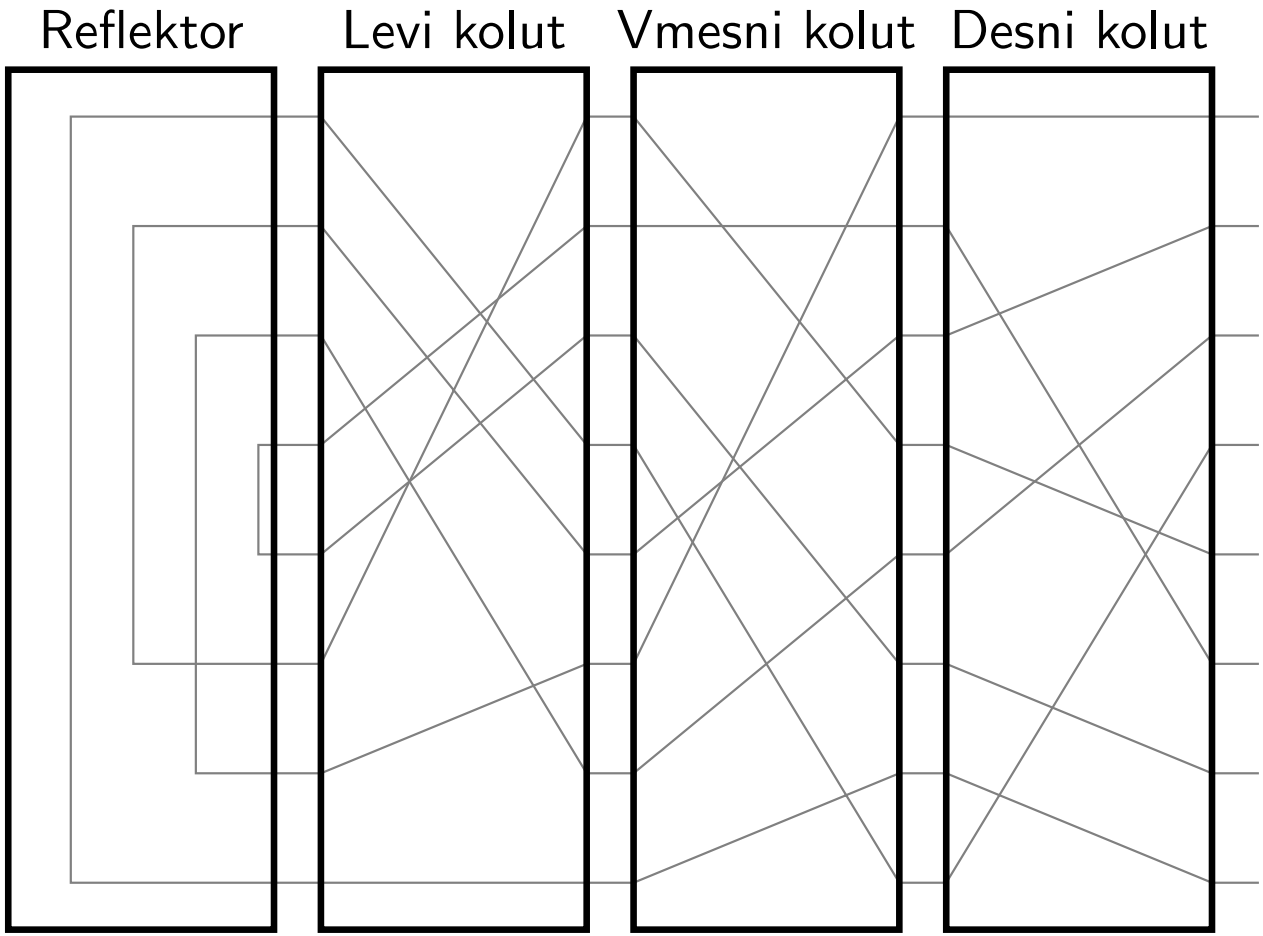


Princip delovanja

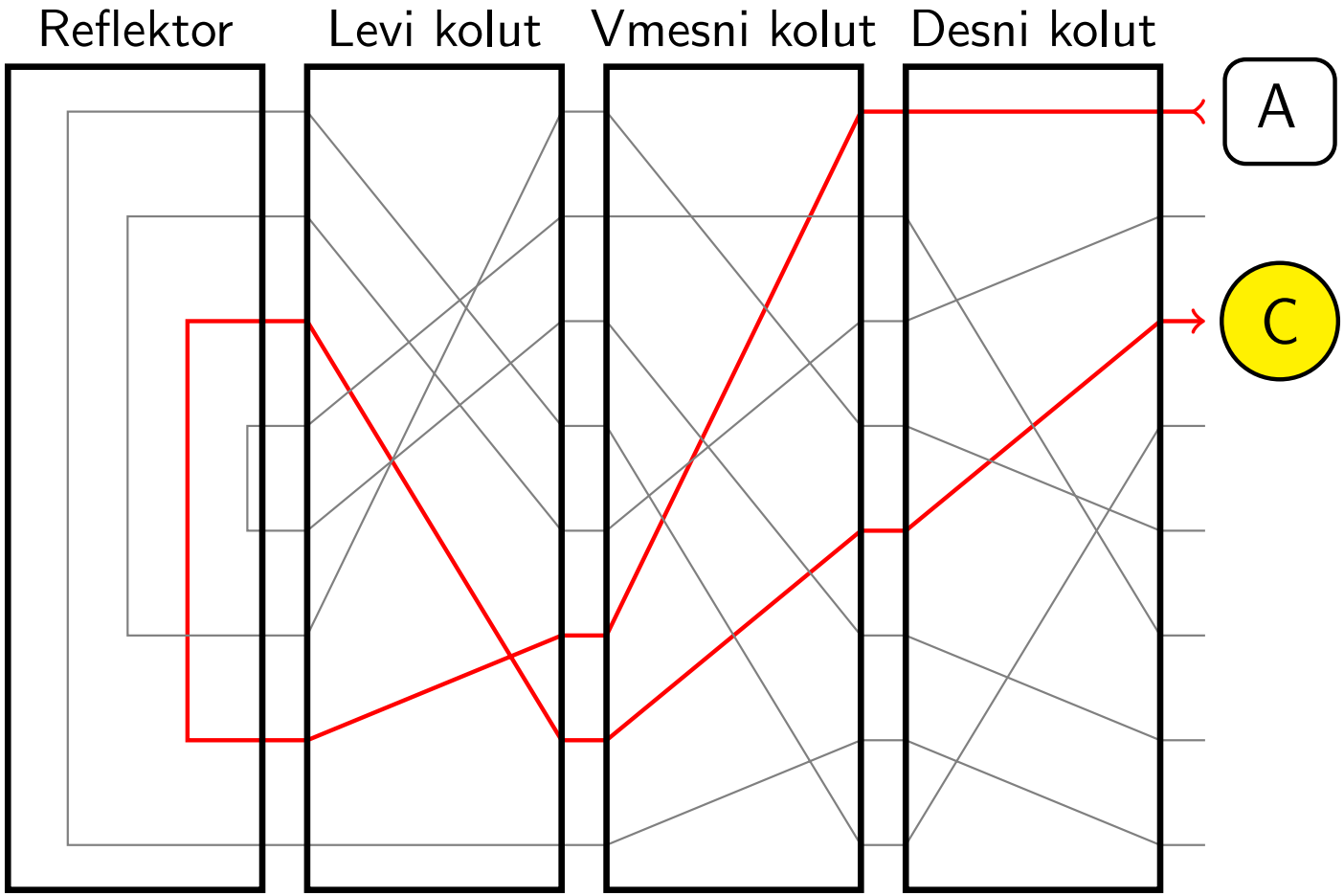
Po pritisku tipke se desni kolut pomakne za eno mesto.



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

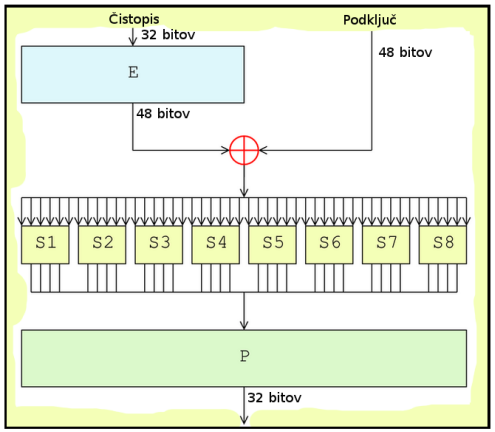
Nastavljeno za vsako sporočilo:

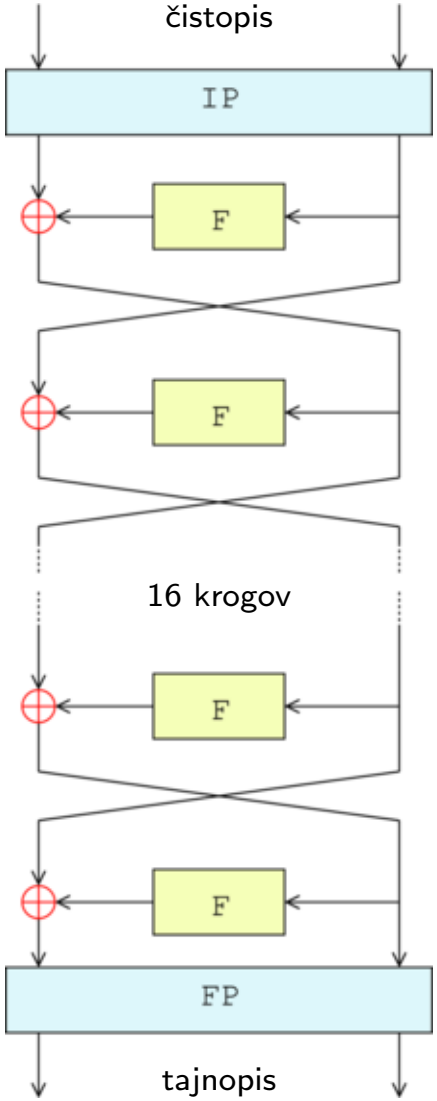
- začetni položaj kolutov $\Rightarrow$ 17576 možnosti

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

Primeri: 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:

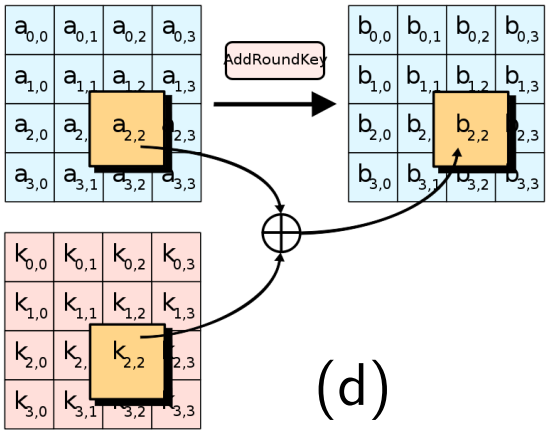




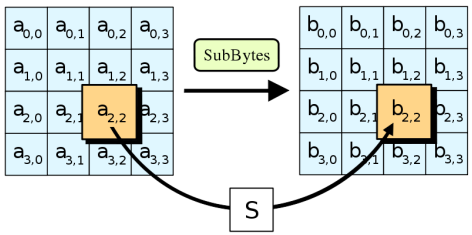
[a]National Security Agency

Primeri: AES-128, -192, -256

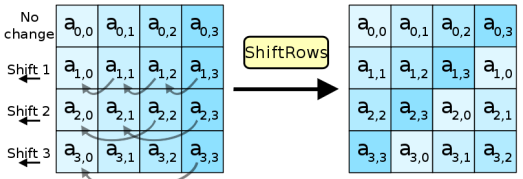
- Advanced Encryption Standard
- Izbran na javnem razpisu NIST
- 1997 pričetek izbora
- 1999 izbranih 5 finalistov
- 2001 objavljen zmagovalec
- Zaporedje korakov:
  $d \longrightarrow (a, b, c, d) \times k \longrightarrow a, b, d$



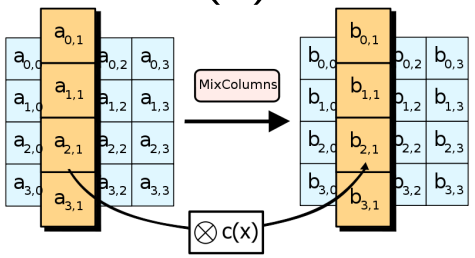
(a)



(b)



(c)



Lastnosti na primeru

Blaž in Ana se vnaprej dogovorita za skupni ključ, ki ga ne pozna nihče drug. S tem ključem lahko tako šifrirata kot dešifrirata sporočila.

Če Blaž z njim zašifrira pismo, je lahko prepričan, da ga lahko dešifrira le Ana.

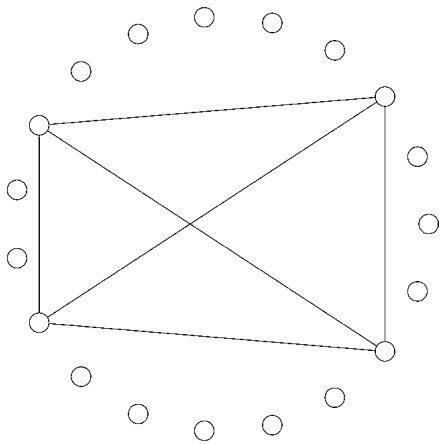
Hkrati pa je tudi Ana zadovoljna, saj je prepričana, da ji je pismo lahko poslal le Blaž.

Problemi

- Skupni 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.

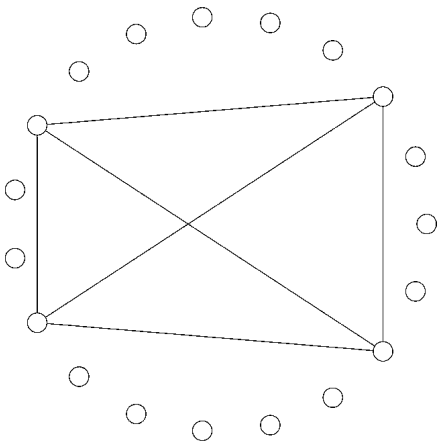
Problemi

- Skupni 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.

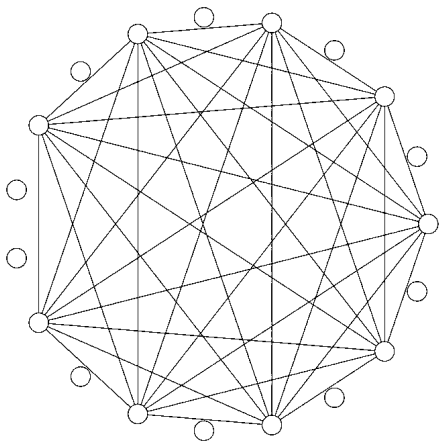


Problemi

- Skupni 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.



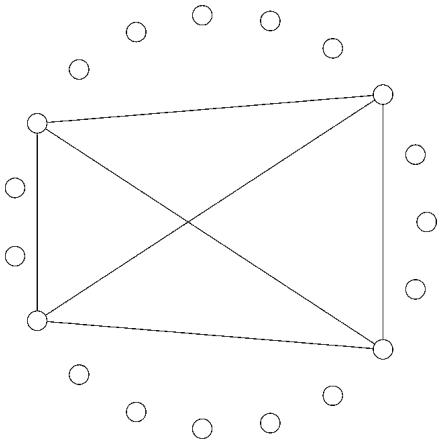
4/6



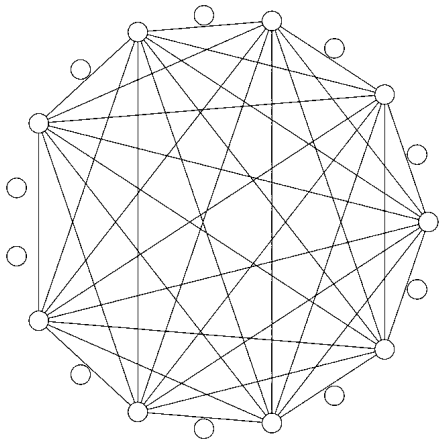
9/36

Problemi

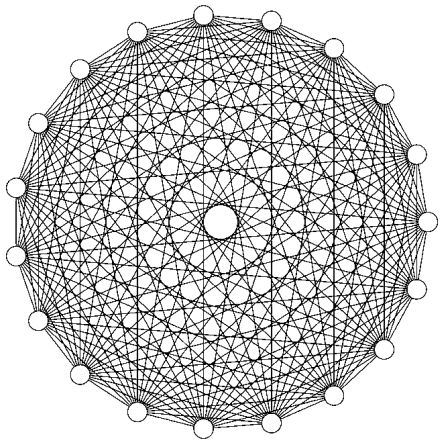
- Skupni ključ mora biti dogovorjen **VNAPREJ**.
- V omrežju z n uporabniki je potrebnih $\binom{n}{2}$ različnih ključev, vsak uporabnik pa mora hraniti $n-1$ ključev.



4/6



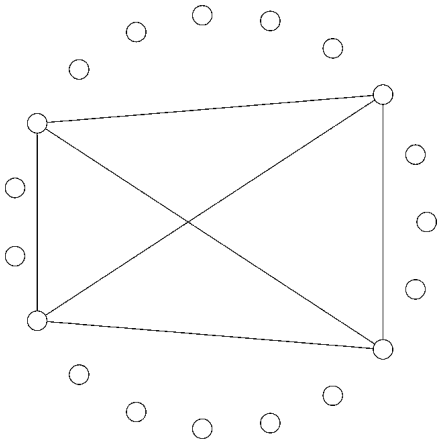
9/36



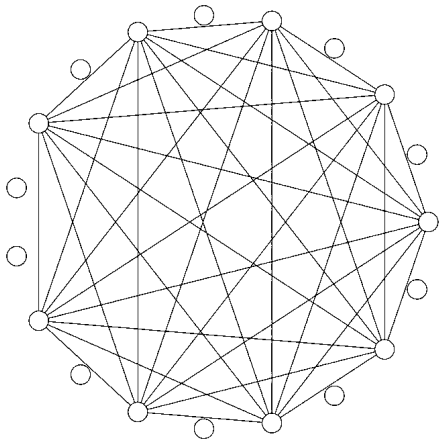
18/153

Problemi

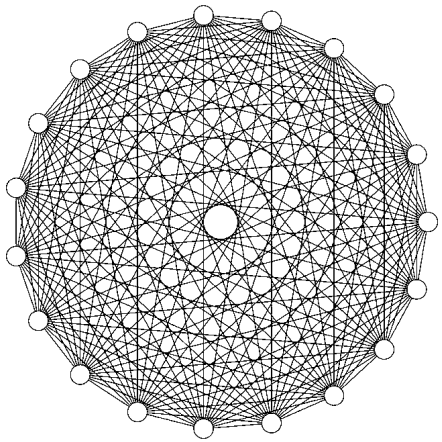
- Skupni ključ mora biti dogovorjen **VNAPREJ**.
- V omrežju z n uporabniki je potrebnih $\binom{n}{2}$ različnih ključev, vsak uporabnik pa mora hraniti $n-1$ ključev.



4/6



9/36



18/153

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

Kratka zgodovina kriptografije

- Osnove kriptografije
- Klasično tajnopisje
- Simetrična kriptografija
- **Kriptografija z javnimi ključi**
- Kriptoanaliza

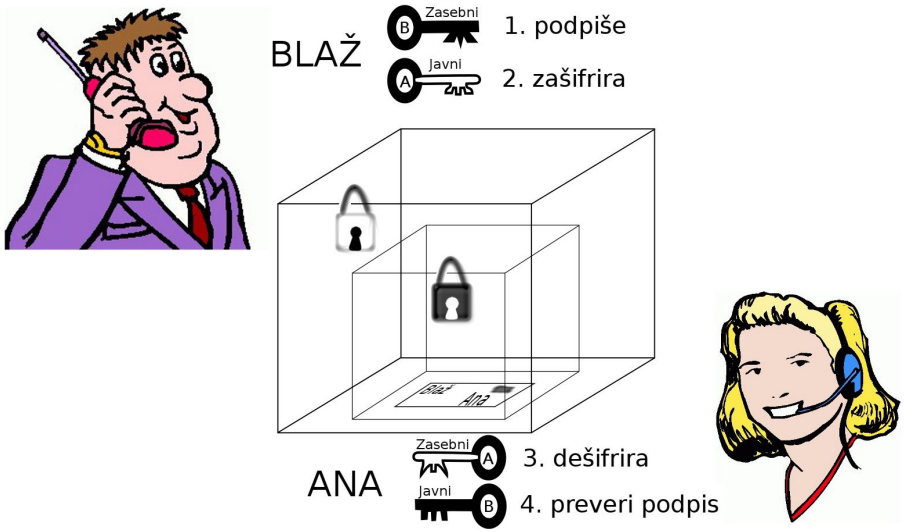
Osnove


- 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

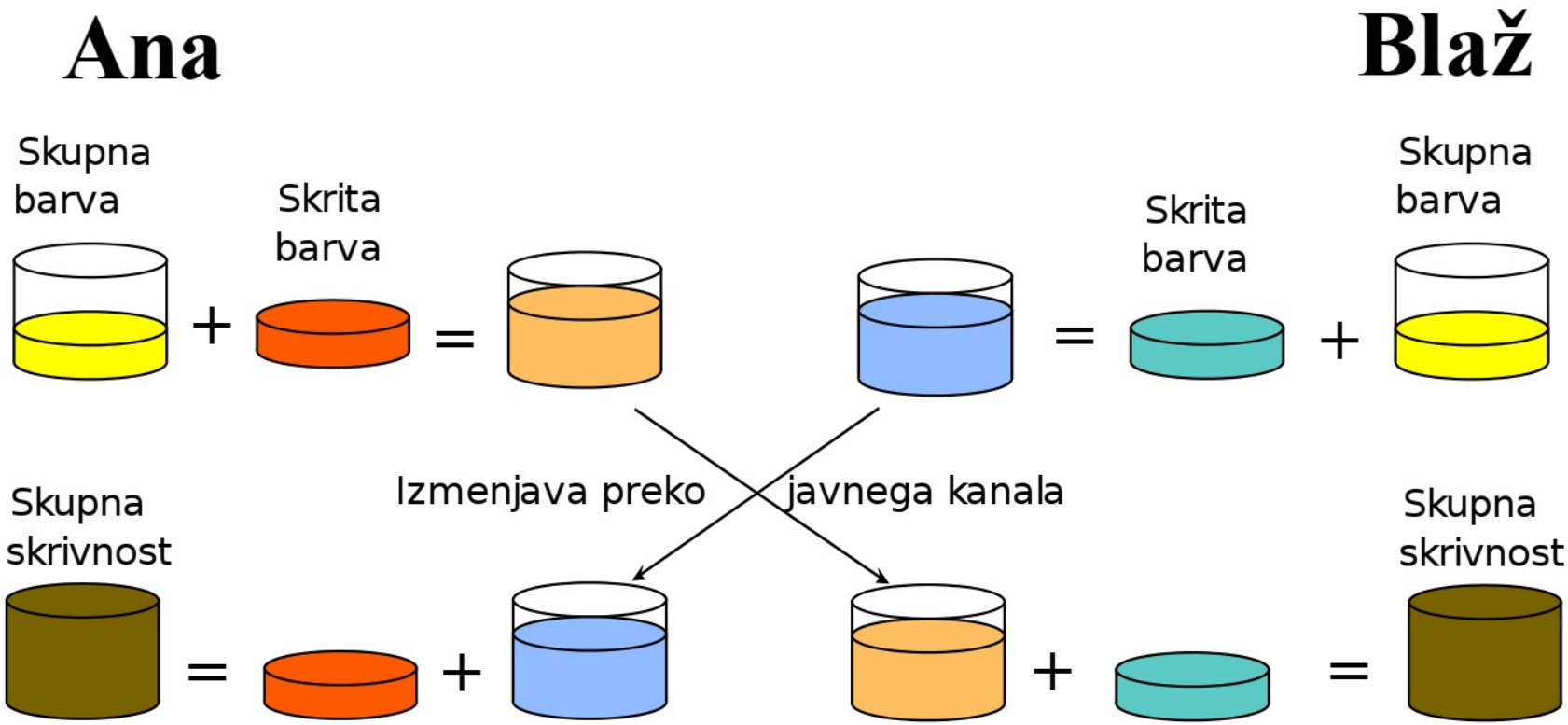
Blaž pošlje Ani podpisano zasebno pismo:

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



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

Diffie-Hellmanova izmenjava ključev – grafično



Diffie-Hellmanova izmenjava – matematično

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

Diffie-Hellmanova izmenjava – matematično

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

naključno izbere

a, $0 < a < n$

Diffie-Hellmanova izmenjava – matematično

a

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

naključno izbere

a, $0 < a < n$

Diffie-Hellmanova izmenjava – matematično

a

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

izračuna g^a

Diffie-Hellmanova izmenjava – matematično

a, g^a

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

izračuna g^a

Diffie-Hellmanova izmenjava – matematično

a, g^a

Skupni parametri: $g \in G$, $g^n = 1$

Ana

Blaž

pošlje g^a Blažu $\xrightarrow{\quad g^a \quad}$

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Oskar

g^a

Skupni parametri: $g \in G$, $g^n = 1$

g^a

Blaž

g^a

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a

Blaž

g^a →

naključno izbere

b, $0 < b < n$

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b

Blaž

$$g^a \longrightarrow$$

naključno izbere

b, $0 < b < n$

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b

Blaž

g^a →

izračuna g^b

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b, g^b

Blaž

$$\xrightarrow{\quad g^a \quad}$$

izračuna g^b

Diffie-Hellmanova izmenjava – matematično

a, g^a

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b, g^b

Blaž

g^a →

← g^b

pošlje g^b Ani

Diffie-Hellmanova izmenjava – matematično

a, g^a, g^b

Ana

Oskar

g^b

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b, g^b

Blaž

g^a

g^b

Diffie-Hellmanova izmenjava – matematično

a, g^a, g^b

Ana

Skupni parametri: $g \in G$, $g^n = 1$

g^a, b, g^b

Blaž

g^a →

← g^b

izračuna $(g^b)^a$

izračuna $(g^a)^b$

Diffie-Hellmanova izmenjava – matematično

$a,\ g^a,\ g^b$

Ana

Oskar

g^a  g^b

Skupni parametri: $g \in G,\ g^n = 1$

$g^a,\ b,\ g^b$

Blaž

g^a →

← g^b

g^{ab}

Skupni ključ

g^{ab}

g^{ab}, a, b morajo ostati skriti!

Matematično ozadje

Glede na matematični problem, na katerem temeljijo sistemi javne kriptografije, se le-ti 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).

Problemi RSA

- Potrebujemo veliki praštevili, javni ključ je njun produkt n
- Če znamo faktorizirati n, je sistem razbit
- 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)
- Za dolgoročno varnost potrebujemo vsaj 15000 bitov (4500 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**[1]	**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
256	$2^{256} \approx 1{,}2 \times 10^{77}$	$\approx 1{,}8 \times 10^{63}$ let	$\approx 1{,}8 \times 10^{57}$ let

Starost vesolja je ocenjena na $13{,}7 \times 10^9$ let.
Število atomov v vidnem vesolju je ocenjeno na 10^{80}.

[1] v povprečju moramo pregledati 1/2 ključev

Kratka zgodovina kriptografije

- Osnove kriptografije
- Klasično tajnopisje
- Simetrična kriptografija
- Kriptografija z javnimi ključi
- **Kriptoanaliza**

Kaj je kriptoanaliza?

- Razbijanje kriptosistemov
- Razvijala se je hkrati s kriptografijo
- V preteklosti dostikrat tajna
- Tudi danes ne vemo, če je vse javno znano
- Uporablja močna matematična orodja

Držimo se **Kerckhoffsovega principa** (1883):

> *Nasprotnik pozna kriptosistem oziroma algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.*

Kriptoanaliza enoabecednih šifer

- Pomagamo si s frekvencami črk (število pojavitev)
- Slovenska abeceda, v %:

E	10,707	L	5,266	V	3,764	Z	2,103	H	1,047
A	10,466	S	5,053	K	3,704	B	1,939	Š	0,996
O	9,084	R	5,010	D	3,390	U	1,879	C	0,662
I	9,042	J	4,675	P	3,374	G	1,638	Ž	0,646
N	6,328	T	4,329	M	3,305	Č	1,483	F	0,110

- Za dani tajnopis izračunamo frekvence črk, ki nastopajo
- S pomočjo tega lahko že uganemo nekaj črk, določimo tudi skupine

- Pomagamo si lahko tudi z dvojčki ...

JE	2,379	IL	1,340	LA	1,232	ST	1,118
SE	1,528	NI	1,291	NA	1,138	AJ	1,111
IN	1,442	AL	1,251	PO	1,135	AS	1,092

- ... in trojčki

BIL	0,395	PRI	0,343	ALI	0,306
EJE	0,391	ILA	0,337	NJE	0,288
AKO	0,383	OST	0,333	STA	0,288
AJE	0,369	PRE	0,324	SEJ	0,287

http://simonsingh.net/The_Black_Chamber/substitutioncrackingtool.html

Kriptoanaliza Vigenèrjeve šifre

- Test Kasiskega (1863): Poiščemo dele tajnopisa, ki se ujemajo. Izračunamo razdalje med njihovimi začetki. Dolžina gesla deli največji skupni delitelj teh razdalj.
- Friedman, 1920: indeks sovpadanja – verjetnost, da sta naključno izbrana elementa besedila enaka
- Če se neka črka pojavi f-krat v besedilu dolžine n, je njen indeks sovpadanja

$$\frac{\text{ugodni pari}}{\text{vsi pari}} = \frac{\binom{f}{2}}{\binom{n}{2}} = \frac{f(f-1)}{n(n-1)}$$

- Indeks sovpadanja besedila je vsota indeksov posameznih črk (f_i je frekvenca črke i, n je dolžina besedila):

$$IC = \sum_{i=1}^{25} \frac{f_i(f_i-1)}{n(n-1)}$$

Kriptoanaliza Vigenèrjeve šifre, nadaljevanje

- Če je p_* pričakovana verjetnost slovenske črke $*$, je $\frac{d}{n} \approx \frac{d-1}{n-1} \approx p_*$ in indeks sovpadanja je približno

$$p_{\mathrm{A}}^2 + p_{\mathrm{B}}^2 + \cdots + p_{\check{\mathrm{Z}}}^2 \approx 0{,}063$$

- Za običajno substitucijsko šifro je indeks sovpadanja tudi pribl. 0,063, saj samo permutiramo člene vsote
- Za povsem naključne črke dobimo

$$\frac{1}{25^2} + \cdots + \frac{1}{25^2} = 0{,}04$$

- Na ta način lahko uganemo dolžino ključa ter sam ključ

Primer

Prestregli smo sporočilo

GVČJUOECDFHŠTLRNTCNNCROEZFCNRMRZČIAŽNJAISOTDAVLNŠCPDLVSZSKVNB
KOKBLKZŠCNŠCIAGTLDŠUFCDTVVŠGBAŽCCSEŽJIČŠVMSIKIAŽIIČSZIBIRAAŽI
EEIHAAŽNVISOTŠVRRŠZSTAEOKDGFVFIRAŽNOIŽIIPDČCVŠZMRNVCNDALLSIKS
ANDAGŽKCNZVRNFKOGDJAINNIKŽAIKNAJŠCLBZUCIČLFSINGŠŠFOAČNZEHTVLJ
LGEDMOEKIIAZGKJZRŠSNZCBŠČHAOUVGDCRIČUGUONTEČEOTČSŽEGŽOEGVCHBŠ
VLŠTVKDBLTFŽHUASMRZZVŠNFCSŠUBAFŠVZEIOECCCOLBIIČCCMFNHEBGTLDJK
ICPIAGŽJPJCRIINJEČIJIFEKECINACGBAŽ

Našli smo dva niza, ki se ponovita: AAŽ in SIK z razmikoma 8 in 76. Največji skupni delitelj je 4. Izračunajmo sedaj še indeks sovpadanja, če vzamemo vse oz. vsako drugo, tretjo, ..., šesto črko:

1 [GVČJ . . .]: 0,045
2 [GČUE . . .]: 0,052 0,047
3 [GJEF . . .]: 0,045 0,046 0,046
4 [GUDT . . .]: 0,053 0,064 0,070 0,061
5 [GOHN . . .]: 0,039 0,049 0,039 0,045 0,052
6 [GETN . . .]: 0,050 0,051 0,057 0,045 0,049 0,041

Primer, nadaljevanje

Ker so indeksi sovpadanja blizu 0,063 samo pri dolžini 4, je dolžina gesla res najverjetneje 4. Izračunajmo še frekvence posameznih črk za ta štiri podzaporedja:

GUDT ... $2, 4, 8, 3, 2, 3, 3, 6, 0, 10_{\mathrm{A}}, 1, 0, 3, 1, 10_{\mathrm{E}}, 0, 1, 2, 6, 5, 6, 6, 3, 6, 9$

VOFL ... $2, 3, 12_{\mathrm{E}}, 0, 1, 0, 5, 3, 4, 8, 6, 9, 6, 3, 3, 10, 0, 6, 1, 1, 2, 0, 12_{\mathrm{A}}, 2, 1$

ČEHR ... $16_{\mathrm{A}}, 2, 3, 1, 1, 12_{\mathrm{E}}, 0, 1, 2, 13, 2, 3, 5, 2, 3, 4, 3, 6, 6, 2, 5, 2, 5, 1, 0$

JČSN ... $6, 3, 5, 9, 10, 4, 5, 6, 1, 5, 3, 4, 1, 0, 10_{\mathrm{A}}, 2, 0, 0, 2, 12_{\mathrm{E}}, 0, 0, 0, 7, 5$

Ker imata A in E najvišjo frekvenco in sta 5 črk narazen, iščemo dve visoki frekvenci s tem razmikom (gledamo ciklično). V vsaki vrstici se to zgodi samo na enem mestu. Od tod takoj dobimo geslo "IVAN".

Primer, nadaljevanje

Lahko pa izračunamo

$$M_g = \sum_{i=1}^{25} \frac{p_i f_{i+g}}{n'},$$

kjer je $n' = \frac{d}{\ell}$ in ℓ dolžina gesla. Če se g ujema s črko gesla, potem pričakujemo, da bo M_g blizu 0,063 (saj se v tem primeru f_{i+g}/n' približno ujema s p_i), sicer pa bo manjši. Če tabeliramo vrednosti za M_g in poiščemo največje vrednosti, ravno tako dobimo geslo “IVAN”.

Primer, nadaljevanje

i	Vrednost $M_g(y_i)$								
	A/I/S	B/J/Š	C/K/T	Č/L/U	D/M/V	E/N/Z	F/O/Ž	G/P	H/R
1	0,213	0,144	0,237	0,157	0,264	0,234	0,177	0,192	0,146
	0,388	0,194	0,167	0,213	0,178	0,284	0,191	0,177	0,198
	0,205	0,273	0,179	0,175	0,222	0,204	0,252		
2	0,275	0,231	0,365	0,155	0,231	0,247	0,287	0,279	0,203
	0,212	0,305	0,244	0,304	0,286	0,169	0,254	0,165	0,348
	0,301	0,194	0,205	0,186	**0,484**	0,205	0,203		
3	**0,613**	0,141	0,186	0,194	0,304	0,373	0,129	0,246	0,282
	0,331	0,340	0,256	0,284	0,299	0,239	0,309	0,416	0,231
	0,225	0,234	0,481	0,301	0,217	0,153	0,176		
4	0,201	0,188	0,233	0,226	0,319	0,264	0,188	0,223	0,181
	0,313	0,294	0,202	0,186	0,202	**0,476**	0,223	0,205	0,197
	0,229	0,375	0,207	0,171	0,203	0,238	0,318		

Primer, zaključek

Dešifrirano besedilo (z vstavljenimi presledki in ločili) se glasi:

Začul sem tihe korake na stopnicah. Prišla je mati; stopala je počasi in varno, v roki je nesla skodelico kave. Zdaj se spominjam, da nikoli ni bila tako lepa kakor v tistem trenutku. Skozi vrata je sijal poševen pramen opoldanskega sonca, naravnost materi v oči; večje so bile in čistejše, vsa nebeška luč je odsevala iz njih, vsa nebeška blagost in ljubezen. Ustnice so se smehljale kakor otroku, ki prinaša vesel dar.
Jaz pa sem se ozrl in sem rekel z zlobnim glasom:
»Pustite me na miru! ... Ne maram zdaj!«

Vprašanja

Povezave in dodatne informacije na

http://lkrv.fri.uni-lj.si/