KAJ, ZAKAJ, KAKO?

2.del

Kaja Vidmar

March 29, 2010

1 UVOD

Drugi del knjige Kaj, Zakaj, Kako? se spušča v svet pravih šifer. Predstavi nam osnovne postopke šifriranja in odšifriranja od enostavne Cezarjeve šifre pa vse do zapletenejše Vigenèrjeve šifre.

Za ohranjanje skrivnosti skrivanje sporočil ni bilo dovolj dobro. Izkazalo se je, da je premalo varno. Zato smo sporočila poskusili zakleniti. Prvo poglavje nas vodi do spoznanja, da je šifriranje sporočil podobno zaklepanju ključavnice s ključem. Opisana je tudi enostavna naprava za šifriranje Skital in pa Cezarjeva šifra.

Naslednje poglavje govori o zamenjalnih šifrah ter o šifri, v kateri premešamo črke odprtega besedila medseboj. Opisan je tudi postopek imenovan frekvenčna analiza, s katerim lahko brez poznavanja ključa iz kriptograma ugotovimo morebitno odprto besedilo.

Nato nadaljujemo s Vigenèrjevo šifro, ki namesto ene menjalne abecede uporablja več le teh. Povemo, zakaj so zmotno mislili, da je ta šifra popolnoma varna in nakažemo način, kako jo lahko razvozlamo.

Zadnje poglavje je zgodba o kraljici Mariji Stuart, ki prikazuje, kako pomembna je varnost šifer.

Pomen oznak:

- Zanimivost. Razlaga, pomembno.
- Razlaga. Pomembno.
- ☞ Zapomni si, opomba, ugotovitev
- ✎ Naloga, kako uporabimo tabelo
- ❀ Razložena beseda
- ☞ Poišči razlago
- ✓ Rešitev naloge

2 KLJUPUČ IPIN KLJUPUČAPAVNIPICAPA

Sčasoma so ugotovili, da samo skrivanje besedil ni dovolj, ter da lahko nasprotnik hitro najde naš način skrivanja. Tako se je razvilo danes zelo poznano KERCKHOFFOVO NAČELO, ki pravi, da varnost kriptograma ne sme biti odvisna od načina šifriranja, saj le tega nasprotnik pozna, ter da mora vsa varnost temeljiti na KLJUČU šifriranja, ki pa je nasprotniku neznan.

✎ Poznaš ključ, po katerem je šifriran naslov poglavja?

Tudi skrivni jeziki so ključ šifriranja. Če ne veš, v katerem jeziku je sporočilo napisano, ga ne moreš prebrati. Ko pa najdeš ustrezni skrivni jezik, se ga naučiš in besedilo hitro prebereš. Ključ je torej namig, ki nam omogoča razvozlanje šifre.

Čas je, da poiščemo nove, varnejše načine ohranjanja sporočil v tajnosti.

❀ **TAJNOST** - pomeni ohranjanje skrivnosti, če je nekaj tajno, potem je skrito širši javnosti
❀ **KRIPTOGRAM** - zašifrirano, skrito besedilo
❀ **KLJUČ** - beseda, geslo, ki ga uporabimo pri šifriranju, če ga poznamo, je razvozlanje šifre hitrejše

Načini ohranjanja tajnosti:

- ☞ pogovor/zapis v tajnem jeziku
- ☞ zapis sporočila v drugačni abecedi
- ☞ kodiranje besedila
- ☞ šifriranje besedila

❀ **ŠIFRA** - šifra je način skrivanja sporočila (kjer vsaki črki abecede posebej spremenimo pomen, po nekem ključu)
❀ **ŠIFRIRANJE** - postopek preoblikovanja sporočila s pomočjo šifre v obliko, ki ni razumljiva vsakomur, obratni postopek imenujemo ODŠIFRIRANJE
❀ **ODPRTO BESEDILO** - besedilu, ki ni zakljenjeno, šifrirano pravimo odprto ali pa tudi PROSTO besedilo

Zaklepanje sporočil

Z zaklepanjem sporočila povečamo stopnjo varnosti in bolje ohranimo tajnost. Kajti malo verjetno je, da bo neznana oseba hitro našla ključ za odklepanje sporočila.

Sporočilo torej »zaklenemo«, da ga drugi ne morejo prebrati.

Na primer: Ana vsak dan pridno piše svoje misli, sporočila v dnevnik. Da ji dnevnika ne prebere brat Jure, ga zaklene s ključavnico, ključ pa spravi na skrivno mesto, ki ga pozna samo ona.

☞ Slabost Aninega zaklepanja dnevnika je v tem, da če Jure najde ključ, lahko preprosto odklene dnevnik in prebere sporočila in misli v njem. Zato raje sporočila zaklepamo s šifriranjem. To je, besedilo preoblikujemo tako, da ga nihče ne zna prebrati. To lahko naredimo tako, da nekako zamenjamo pomen črk, vrstni red črk,...
Ideji, kako zamenjamo pomen, vrstni red črk, pravimo ključ, in ta je znan samo nam. Za postopek kako smo prvotno besedilo spreminjali v šifrirano, pa predpostavimo, da je vsem znan.

Skital

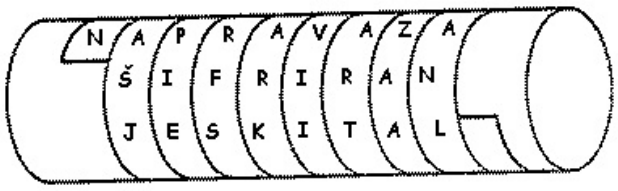
Skital je ena prvih naprav za šifriranje besedila. Uporabljali so ga že v Šparti okoli leta 475 p. n. št. Pošiljatelj in prejemnik sta imela palico v obliki valja z enakim polmerom. Pošiljatelj je okoli palice navil trak iz pergamenta in nanj po dolžini napisal sporočilo. Nato je trak odvil in ga poslal prejemniku. Ta je trak ovil na palico enakega polmera in prebral sporočilo. Polmer je torej ključ tega šifrirnega postopka.

✎ Naredi sam

Potrebujemo:

- 1 rolo od papirnatih brisač
- list A4 papirja
- svinčnik

Navodilo: List A4 papirja razreži po dolžini na trakove široke približno 1cm. En trak navij okoli role od papirnatih brisač in nanj po dolžini napiši sporočilo. Nato odvij trak.



Cezarjeva šifra

To šifro je uporabljal že Gaj Julij Cezar (približno 100 pr. n. št. - 44 pr. n. št.). Zato jo imenujemo ☞Cezarjeva šifra.

Izberemo si eno črko na primer K. Zavrtimo abecedo tako, da se začne pri K. Dobimo abecedo: K L M N O P R S Š T U V Z Ž A B C D E F G H I J.

Nad to abecedo napišemo navadno abecedo. Torej:

original	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
zamenjava	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

V zgornji abecedi (to je originalu) vzamemo črko, ki jo šifriramo, in pogledamo v spodnjo abecedo, v katero črko se zašifrira. Namesto originalne črke zapišemo črko, ki ji pripada v zamenjevalni abecedi.

Iz besedila: "Danes je lep dan". Dobimo: OKAPDJPZPCOKA.

(Črka D se preslika v O, A v K, N v A...)

Izbrana črka je naš ključ šifriranja. Pove nam, kako moramo zavrteti abecedo, da lahko šifrirano besedilo odšifriramo.

☞ Navada je pisati kriptograme z velikimi črkami, prosto (odprto) besedilo pa z malimi, presledke in ločila pa ponavadi izpuščamo.

Tudi odšifriranje poteka podobno. Le abecedi zamenjamo. Spodnja postane zgornja in zgornja postane spodnja:

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
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

Skrita matematika za Cezarjevo šifro

1. Črke v abecednem vrstnem redu oštevilčimo (začnemo z 1):

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Besedilo spremenimo v številke. V primeru besedila: "Danes je lep dan", dobimo:

   "5 1 15 6 19 11 6 13 6 17 5 1 15".

   (Napisani presledki so za to, da ločimo eno in dvomestna števila med seboj.)

   Recimo, da je naš izbrani ključ črka K̄=12. Ker želimo imeti črko K na prvem mestu abecede, moramo originalno besedo zavrteti za 11 mest (za ključ A̲ ne zavrtimo abecede, za ključ B̲ jo zvrtimo za 1 črko, za ključ C̲ jo zavrtimo za 2 črki, ...). Število, za koliko mest zavrtimo abecedo, prištejemo vsakemu številu našega besedila:

5	1	15	6	19	11	6	13	6	17	5	1	15
+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11
==	==	==	==	==	==	==	==	==	==	==	==	==
16	12	26	17	30	22	17	24	17	28	16	12	26

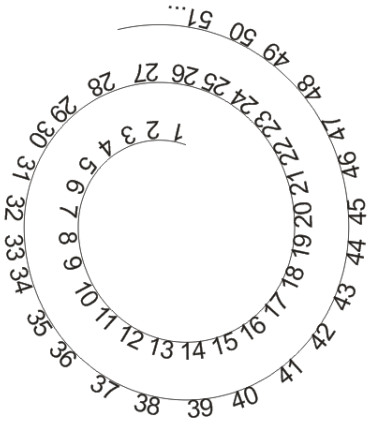
   ☞Opazimo, da nekatere številke nimajo pripadajočih črk. Natančneje, števila večja od 25 nimajo pripadajočih črk.

   ☞ Opazimo tudi, da nam števila manjša od našega izbranega ključa manjkajo. Zato številom, ki jim manjkajo črke pripišemo po velikostnem vrstem redu (najmanjšemu najmanjše) števila, ki nam manjkajo. Na primer, številu 26 pripišemo število 1, 27 pripišemo število 2 in tako dalje.

3. Dobimo:

5	1	15	6	19	11	6	13	6	17	5	1	15
+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11	+11
==	==	==	==	==	==	==	==	==	==	==	==	==
16	12	1	17	5	22	17	24	17	3	16	12	1

   Za lažjo predstavo si lahko predstavljamo števila od 1 do 25 napisana v krogu. Ko pridemo do števila 25 enostavno nadaljujemo naprej z 1:

   To počnemo avtomatično, ko gledamo na uro s kazalci. Kazalci lahko kažejo le 12 ur, dan jih ima pa 24. Vendar popoldne vemo, da če ura kaže 4, da je ura 16h. V resnici računamo ostanke pri deljenju s številom 12 (v prejšnjem primeru s številom 25), ne da bi se tega zavedali.

4. Sedaj ko imamo vse številke med 1 in 25 , številke spremenimo nazaj v črke. In dobimo kriptogram: "O K A P D J P Z P C O K A".

A le to šifro se lahko hitro razbije in kriptoanalitiki, to so razbijalci šifer, z njo niso imeli težkega dela. Ko so enkrat ugotovili, da gre za zamik črk, ni bilo težko odkriti za koliko so črke zamaknjene.

Razbitje Cezarjeve šifre

Kriptoanalitiki so enostavno preiskusili vse možne ključe in tako kmalu dobili rešitev. Namreč možnih ključev je le toliko, kolikor je črk v abecedi - to je 25.

Če ključ ni pravilen, besedilo odšifrirano z njim, ne bo imelo smisla. Če pa je ključ pravilen, bo besedilo tvorilo neko smiselno sporočilo.

❀ Kriptoanalitik - razbijalec šifer

✎ Odšifrirajmo OUMTŽŠDSDPMŽMO:

- Prvi možni ključ A izpustimo, saj nam abecede ne spremeni.
- Naslednji in prvi uporabni ključ je 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
  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

  Če poskusimo odšifrirati besedilo OUMTŽŠDSDPMŽMO, dobimo: ntlšzsčrčolzln. Kar ni nič smiselnega, tako vemo, da ključ B ni pravi.
- Poiskusimo z naslednjim ključem 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
  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

  Tokrat dobimo: mšksvpcpcnkvkm. Kar tudi ni smiselna beseda.
- Naslednji ključ je 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
  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

  Dobimo: lsjruobobmjujl. Tudi tokrat nismo imeli sreče.
- Nadaljujemo s ključem 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
  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

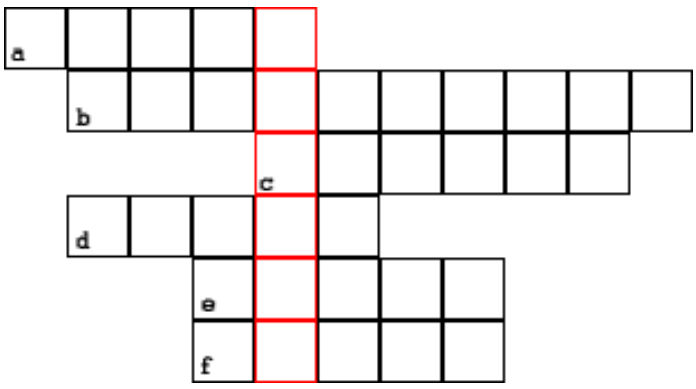
  Dobimo: kriptoanalitik. In našli smo našo rešitev.

Ponovimo

- **KERCKHOFFOVO NAČELO** pravi, da varnost kriptograma ne sme biti odvisna od načina šifriranja, saj le tega nasprotnik pozna, vsa varnost mora temeljiti na KLJUČU šifriranja, ki pa je nasprotniku neznan.
- **KRIPTOGRAM** - kriptogram je zašifrirano sporočilo
- Navada je pisati kriptograme z velikimi črkami, prosto (odprto) besedilo pa z malimi, presledke pa izpuščamo.
- **TAJNOST** - pomeni ohranjanje skrivnosti, če je nekaj tajno, potem je skrito širši javnosti
- **KLJUČ** - beseda, geslo, ki ga uporabimo pri šifriranju, če ga poznamo, je razvozlanje šifre hitrejše
- **ŠIFRA** - šifra je način skrivanja sporočila (kjer vsaki črki abecede posebej spremenimo pomen, po nekem ključu)
- **ŠIFRIRANJE** - postopek preoblikovanja sporočila s pomočjo šifre v obliko, ki ni razumljiva vsakomur, obratni postopek imenujemo ODŠIFRIRANJE
- **ODPRTO BESEDILO** - besedilu, ki ni zakljenjeno, šifrirano pravimo odprto ali pa tudi PROSTO besedilo
- **KRIPTOANALITIK** - razbijalec šifer

Naloge

1. Kakšno načelo se je razvilo skupaj z razvojem kripotgrafije?
2. Razbij Cezarjevo šifro:
   - ŽKFPŽKFTVK
   - VČTCFBSČKŽ
   - ZBŠDM
3. Križanka
   Navodilo: Rdeči kvadratki, brani od zgoraj navzdol, ti dajo rešitev križanke.
   (a) Če ga poznamo, lahko odšifriramo. Z njim tudi kaj odklenemo.
   (b) Ena izmed izumrlih pisav, pisva s ...
   (c) V kriptografiji je zelo pomembno Kerckhoffovo ...
   (d) Nanj kaj napišemo.
   (e) Če z njim pišemo po papirju, se sporočilo prikaže, ko po njem potrsemo prah.
   (f) Z njim lahko pišemo, rišemo...



3 ZAMENJALNA ŠIFRA in PREMEŠANKA

Cezarjeva šifra ni dovolj varna. Oglejmo si še malo varnejši šifri: zamenjalna šifra in premešanka.

ZAMENJALNA ŠIFRA

Zelo enostavna je tudi zamenjalna šifra. Naredimo si tabelo:

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

Zgornja vrstica predstavlja originalno abecedo, spodnja pa menjalno. V spodnjo vrstico, torej zapisemo črke abecede v poljubnem vrstem redu. Če abecedo le zamaknemo, dobimo Cezarjevo šifro. V naši tabeli se preslika a v M, b v A, ...Za odšifriranje pa smer obrnemo. J se preslika v ž, I v z,..., K v a.

✎ Z dano menjalno abecedo šifrirajmo sporočilo: "ZAMENJALNA ŠIFRA".

- Najprej izpustimo presledke in ločila: ZAMENJALNAŠIFRA
- Nato uporabimo zamenjalno abecedo in šifriramo črko po črko.
  Dobimo: IMVČSPMRSMNOČBM.

✎ Z isto abecedo odšifrirajmo sporočilo: CMPSMMAČTČKM.

- Abecedi obrnemo (menjalna postane original in original postane menjalna abeceda):

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

- Odšifriramo črko po črko. Dobimo: TAJNAABECEDA.
- Po potrebi vstavimo še ločila in presledke. TAJNA ABECEDA.

Uporabljena menjalna abeceda ima popolnoma naključen vrstni red črk. Slabost je,da morata imeti pošiljatelj in prejemnik oba isto abecedo. Ključ take abecede, je kar cela abeceda.

Ponavadi pa se pošiljatelj in prejemnik raje kot za celotno abecedo, dogovorita le za ključno besedo, ki določa abecedo. Poglejmo si na primeru.

✎ Recimo, da je naša ključna beseda, beseda SVINČNIK. Menjalno abecedo sestavimo tako, da na začetek abecede napišemo besedo SVINČNIK brez ponovljenih črk. Napišemo torej SVINČK (drugi N in drugi I smo izpustili, ker smo ju že napisali - abeceda vsebuje vsako črko le po 1x):

original	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
menjava	S	V	I	N	Č	K	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Ostala prosta mesta v abecedi pa napolnimo s preostalimi črkami v pravilnem vrstnem redu (že uporabljene črke SVINČK seveda izpustimo):

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

Postopek šifriranja in odšifriranja poteka popolnoma enako kot prej. Ključna beseda, ki smo si jo izbrali za začetek menjalne abecede, je naš ključ šifriranja.

Posebno mesto v zamenjalnih šifrah ima šifra imenovana Atbash. Menjalna abeceda je abeceda napisana od zadaj naprej:

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

Za razbitje zamenjevalne šifre moramo ugotoviti s kakšno abecedo je zamenjana naša prvotna abeceda. Da bi razbili zamenjevalno šifro, so kriptoanalitiki razvili postopek imenovan frekvenčna analiza.

PREMEŠANKA

Pri tej šifri ne premešamo črk abecede. Temveč premešamo črke odprtega besedila.

- Najprej si izberemo dolžino ključa, ki mora biti manjša ali enaka dolžini odprtega besedila skupaj s presledki. Za besedilo: "Danes-je-lep-dan"(namesto znaka za presledek je uporabljen znak -), mora biti torej ključ krajši ali enak 15. Recimo, da si izberemo dolžino 6.
- To pomeni, da moramo razdeliti besedilo na kose dolžine 6 takole: Danes-, je-lep,-danxy. XY smo dodali, da je tudi zadnji kos dolžine 6.
- Sedaj si naredimo "mešalno tabelo", na primer:

1	2	3	4	5	6
5	3	1	6	4	2

☞ Tabelo beremo tako, da gre prva črka na peto mesto, druga na tretje, tretja na prvo, četrta na šesto, peta na četrto in šesta na drugo mesto.

✎ Takih mešalnih tabel je veliko. Spomni se še kakšne!

- Z uporabo tabele tako dobimo kriptogram (zapisan po kosih dolžine 6 ločenih z vejico): "N-ASDE, -PEEJL, AYDX-N".

☞ Odšifriranje poteka podobno, le da tabelico beremo od spodaj navzgor torej:

5	3	1	6	4	2
1	2	3	4	5	6

Peta črka gre na prvo mesto, tretja na drugo, prva na tretje, šesta na četrto četrta na peto in druga na šesto.

Za razbitje premešanke, moraš v vsaki besedi pravilno razporediti črke, da dobiš smiselno besedo. Če pa besedilo ni napisano po besedah, moramo prej ugotoviti še dolžino ključa, da si lahko zapišemo besedilo po besedah, ter nato premetavamo črke.

✎ Razbijmo NOSKČE.

- Ker ne poznamo dolžine ključa, moramo poskusiti vse možne dolžine. Prva smiselna dolžina ključa je 2.
  - Razbijemo besedo na po 2 črki dolge nize: NS OK ČE.
  - Preiskusimo sedaj možne razporeditve teh črk:

NS	OK	ČE
SN	KO	EČ

  - Ker premešanka vse nize črk premša enako. Sta za dolžino ključa to edini možni besedi. Ker nobena ni smiselna, dolžina ključa 2 ni prava.
- Naslednja možna dolžina ključa je 3.
  - Razbijemo besedo na po 3 črke dolge nize: NSO KČE.
  - Preiskusimo sedaj možne razporeditve teh črk:

NSO	KČE
NOS	KEČ
SNO	ČKE
SON	ČEK
ONS	EKČ
OSN	EČK

  - V 4 vrstici opazimo smiselno besedo SONČEK. Vendar dokler ne preiskusimo vseh možnih dolžin ključev, ne moremo biti prepričani, da je ta beseda naša rešitev. Možno bi bilo, da smo jo našli po naključju.
- Ključa dolžine 4 in 5 zagotovo nista prava, saj imamo premalo črk (nizev dolgih 4 ali 5 črk ne moremo narediti). Ostane nam le še ključ dolžine 6.
  - Ker je beseda NSOKČE dolga 6 črk. Imamo le en niz: NSOKČE.
  - Preiskusimo sedaj možne razporeditve teh črk (napisanih jih je le nekaj, v resnici je vseh možnih razporeditev kar 720):

NSOKČE	NSKOČE	NSČOKE	NSEOKČ	NOSKČE	…
NSOKEČ	NSKOEČ	NSČOEK	NSEOČK	NOSKEČ	…
NSOEKČ	NSKČOE	NSČKEO	NSEČOK	NOSEČK	…
NSOEČK	NSKČEO	NSČKOE	NSEČKO	NOSEKČ	…
NSOČEK	NSKEOČ	NSČEOK	NSEKOČ	NOSČEK	…
NSOČKE	NSKEČO	NSČEKO	NSEKČO	NOSČKE	SONČEK

  - Že v napisanih razporeditveh črk, smo našli še vsaj še eno možno besedo: NOSČEK. In le iz sobesedila bi lahko zagotovo vedeli, katera je prava.
- V resnici je dovolj pregledati vse možne razporeditve črk v najdaljšem možnem ključu (torej toliko kolikor je črk je dolg kriptogram). Vendar pa nam tako izčrpno iskanje vzame veliko časa.

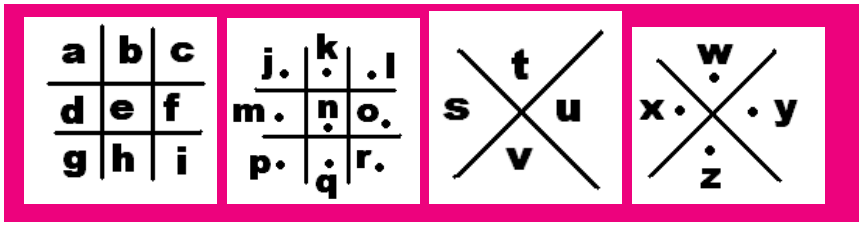
❀ **IZČRPNO ISKANJE** - tako imenujemo postopek iskanja, pri katerem pregledamo vse možne rešitve, za dani primer, bi tako napisali vseh 720 možnih razporeditev teh 6 črk in nato obkrožili vse smiselne besede. Obkrožene besede, nam nato predstavljajo rešitev izčrpnega iskanja.

✎ Koliko časa misliš, da bi porabil, da zapišeš vseh 720 možnih razporeditev črk SONČEK?

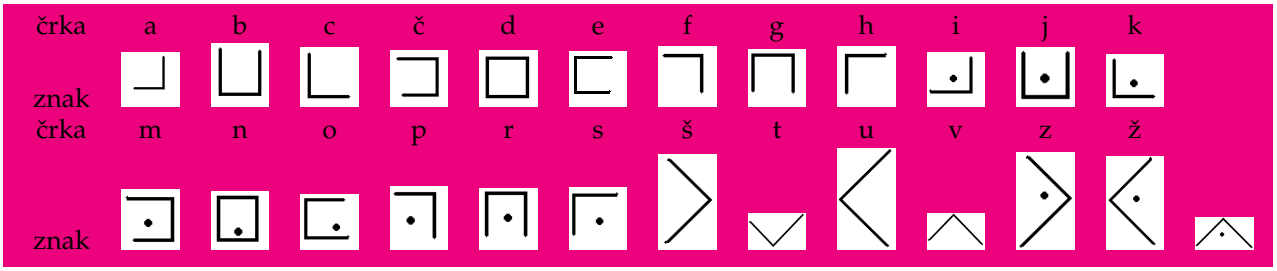
Zato raje začnemo iskanje s manjšimi ključi, in upamo, da kmalu najdemo ustrezno rešitev.

Prostozidarska šifra

Poglej si še naslednjo šifro:



To je posebna vrsta zamenjevalne šifre, črka ni zamenjana s črko, temveč jo zamenja znak. Vsaka črka ima svojo enolično postavitev črt z ali brez pike. Takim šifram pravimo eno abecedne, saj vsako črko nadomesti druga, vendar vsakič ista črka oziroma simbol.



Frekvenčna analiza

Frekvenčna analiza kot orodje uporablja pogostost črk. Z njo lahko razbijemo zamenjevalno šifro, če je le zašifrirano besedilo dovolj dolgo. Pri odšifriranju nam pomagajo razne lastnosti jezika. Pri tem si pomagamo z napotki:

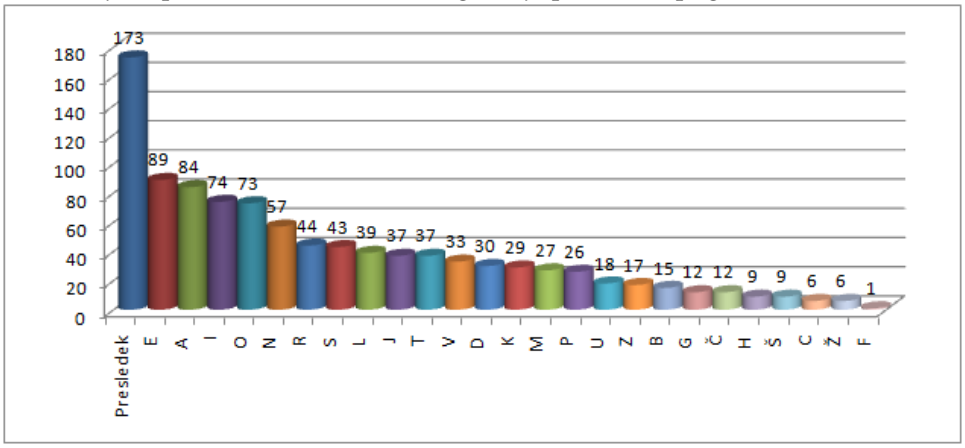
- ☞ Nekatere črke se v jeziku uporabljajo bolj pogosto kot nekatere druge. V slovenščini, se največ uporabljajo samoglasniki e, a, i, najmanj pa soglasniki c, ž, f. Če torej preštejemo število posameznih črk v besedilu, in iz tega izračunamo njihov delež (št. črk / vse črke), lahko ugibamo, katera črka se verjetno preslika v katero.
- ☞ Za začetek predpostavimo, da se črka z največjim deležom preslika v najpogostejšo črko, črka z drugim največjim deležom v drugo najpogostejšo črko v besedilu, ter tako naprej, za vse ostale črke.
- ☞ Nato poskusimo odšifrirati besedilo.
- ☞ Na določenih delih besedila ne dobimo s prvim poskusom vedno smiselnega besedila. Ali nadaljujemo s poskušanjem in razumevanjem preostalega besedila in tako razberemo kakšno besedo več, ali pa poskusimo s kakšnim drugim razporedom črk, tako, da tiste črke, ki so si po pogostosti blizu, ustrezno zamenjamo med seboj.
- ☞ Pri razbijanju šifre nam lahko pomagajo še naslednje jezikovne lastnosti slovenščine in namigi:
  - na začetku besede so najpogostejše črke: N, S, K, T, J, L,
  - ugotovi kateri znaki predstavljajo samoglasnike in kateri soglasnike,
  - v vsaki besedi je vsaj en samoglasnik ali samoglasniški R,
  - v vsaki besedi z dvema črkama je ena črka samoglasnik, druga pa soglasnik,
  - detektivske sreče ni nikoli premalo.

Uporaba frekvenčne analize

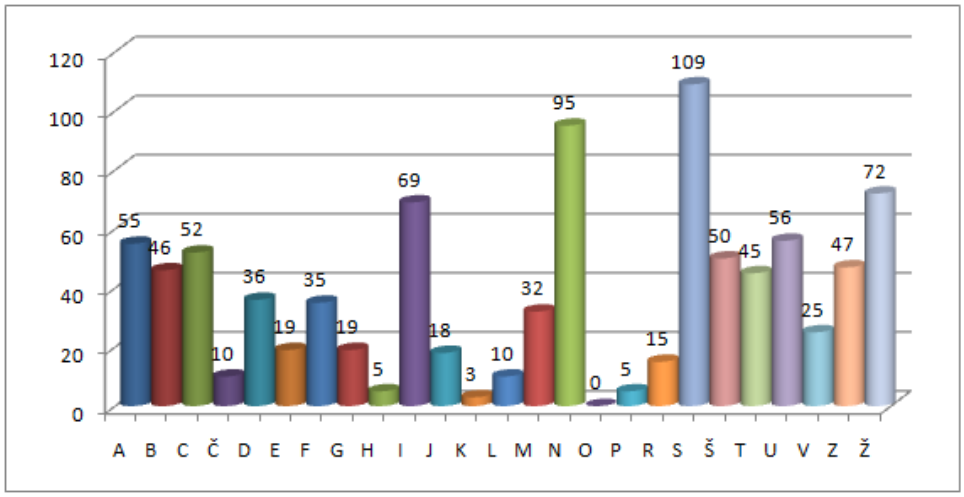
✎ Naslednje besedilo je zašifrirano z zamenjevalno, natančneje Cezarjevo šifro. Kot je v navadi pri šifriranju, so presledki in ločila v besedilu izpuščena. Besedilo je napisano v slovenščini:

ZNTŽLŠNHSFNUFŽUTTSCSŠNZNGZIZCTŽHNUNUABSABIFSDSANLN
ZTŽSGDBNRAEŠCTŽFTSCŽHSFNUSFRSČSKSCBNMSPŽGMIFCITMIZ
ŠNABNVSČUŠNFIUTITŽJSŠSRABNDNZDIUMIJSŠSRUIRTŽEŠNUZI
ŠABNŠŠNAŽCTECSUCAUNGIDSCTŽGSMSVZSTSZŠSRABNCNZNDSDS
IVAITFCNUNZSČUŽDITŽTŽDCSŠNABNMCDIFUŠIUTŽŠNFŽUTUNGN
UCTŽGSMSVZSTŠNGICUSČIUŽMGZŽDBIŠAŽTIZŠNVSCUSUŠNMIŠN
ABSAEŠCTSRZIŽJSCTEUŽFNKGIDŽŠNRSDBŽGJNHIUMŽVŽFFNZMI
BAICŽAEŠCTSCIVŽTŽCDIZŠANTUSMBEPSMIZAICSŠNFŽUTBNTNU
VŽPŽLNJSVSAIECANUŽLNJSŠSRAŽCTECSUABNABSLIDSMICNVAB
SŠIGNZFŽUTAŽDNVJSVNCAECDSUSFRSČŽSZŠIGJSŠSREŠNUSZBN
CŠNFŽUTČNUMŽRSČSKNŽMAEŠCTŽFAŽDBTIUŠNSZBNTNUMŽJNBMI
ZAEŠCTSŠIGCNVFŽUTŽMUŽLSUCNVCNMIJŽVABSŠIGNZSZBIMJSJ
SUFIČABSŠIDNUŠIVSŽMABNDNFBIDIFNZMIBAICNAEŠCTSZSCŽA
ECDSUSABNDNZDIDSZNFNBŠIVNVŽDSDSCSREMŽJNZFŽUTLNJSDS
ŽMABUSJSZICGPBIJSUSZSGZICABSABIFSUANLNZTŽAŽŠMSMŽVŽ
FZNJŽVŽDSŽMABUSFNZMIBAICNFŽUTZSAECDSUŽMPZIDSSZŠSRŠ
NČNZIABNŠABNABSLNFIUIVAITŠIGCNVBNCABSŠIGNZFŽUTSZBN
CRŽLNVJSDSFIČABSŠIDNUŠDŽMIAEŠCTSZSCŽAŽAECDSUSSZFŽU
TCNŠNVŽBIUAŽBIHNZFBZSDSMŽVŽF

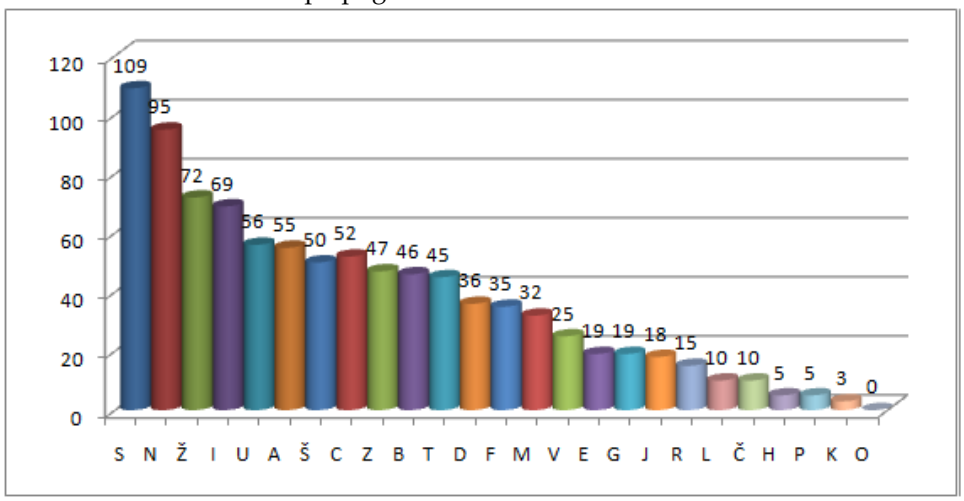
1. Najprej moramo ugotoviti pogostost črk za jezik, v katerem je besedilo napisano.
2. Besedilo je napisano v slovenščini. Na grafu je prikazana pogostost črk v slovenščini:



3. Nato ugotovimo kakšna je pogostost črk v napisanem besedilu. Na grafu je prikazana razporeditev črk v danem zašifriranem besedilu.



4. Črke iz besedila uredimo po pogostosti.



5. Ker vemo, da je zamenjalna abeceda, le zamik originalne, poskušamo uganiti zamik:

   Najpogostejši črki v slovenščini sta, e in a, v besedilu pa S in N. Zato sklepamo, da e, a zamenjata črki S, N, saj za njima sledi kar velik preskok do naslednje črke.

   Zapišemo si vse 4 možne tabele:

(a)

e se preslika v s:	
original	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
zamenjava	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

(b)

e se preslika v n:	
original	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
zamenjava	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

(c)

a se preslika v s:	
original	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
zamenjava	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

(d)

a se preslika v n:	
original	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
zamenjava	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

6. Sedaj pogledamo še najmanj pogoste črke:

   V zašifriranem besedilu, se črka O sploh ne pojavi, zelo redko kdaj pa se pojavijo tudi črke: K, P, H. V slovenščini so najmanj uporabljene črke: f, ž, c, š. In sklepamo, da se črke, O, K, P, H preslikajo v f, ž, c, š zaporedoma.

7. Sedaj pogledamo v naše izbrane tabele, in poskušamo določiti pravo. Prava je tista, ki ima pri najmanj pogostih črkah, najman odstopanj:

   - V tabeli (c) se črka f preslika v Ž, črka ž v R, c v T in š v L. Ker preslikane črke, niso v besedilu med najmanj uporabljenimi, sklepamo, da ta tabela ni prava.
   - V tabeli (d) se črka f preslika v T, črka ž v M, c v P in š v H. Opazimo, da se dve črki preslikata v črki, ki sta v besedilu med najmanj uporabljenimi. A iščemo še boljše ujemanje.
   - V tabeli (a) se črka f preslika v Š, črka ž v L, c v O in š v G. Tudi ta zamik ne ustreza.
   - V tabeli (b) se črka f preslika v O, črka ž v H, c v K in š v Č. In smo našli najboljše ujemanje. Zato s to tabelico poskusimo srečo.

8. Z izbrano tabelo odšifriramo Cezarjevo šifro.

9. Vstavimo presledke in ločila.

Ko odšifriramo besedilo in vstavimo presledke ter ločila, dobimo prvi del zgodbice:

Nekoč je živel volk, ki si je neznansko želel pripraviti pečenko iz treh pujskov, ki so živeli v hišici sredi gozda. Vsak dan je premišljeval, kako bi jih pretental, da bi jih lahko ujel.
Najprej je poskusil splezati skozi dimnik in jih presenetiti, ampak vse le ni šlo tako, kot si je predstavljal. Ko je volk lezel skozi dimnik, je zaslišal od znotraj pokanje. Mislil je, da je pri pujskih na obisku lovec, zato je hitro zbežal domov. Vendar pa so pujski samo kostanj pekli.
Drugi dan pa si je volk rekel: »Mogoče bi mi pa uspelo, če bi jih poskusil prepričati, da sem prijazen volk. Potem bi me spustili v hišo in jaz bi jih ujel.« In res je volk šel do hišice od pujskov. Potrkal je in rekel: »Dober dan pujski, jaz sem volk. Odločil sem se da bom prijazen in rad bi bil vaš prijatelj. A mi odprete vrata?« Vendar pa se pujski niso pustili pretentati: »Ne verjamemo ti. Ti si hudoben volk, če bi ti odprli bi nas zgrabil in iz nas pripravil pečenko. Pojdi domov, ne bomo ti odprli!« Vendar pa se volk ni pustil odgnati in jih je še naprej prepričeval: »Ampak jaz sem res prijazen volk in res hočem biti vaš prijatelj.« Toda pujski niso popustili in volk se je moral poražen vrniti domov.

Tudi dosedaj omenjenih šifer ni tako težko razbiti, še posebno danes ne, ko nam statistiko črk računajo računalniki. Slabost zamenjevalnih šifer je bila predvsem ta, da se ista črka vedno preslika v isto črko zamenjevalne abecede. Zdelo se je, kot da so kriptoanalitiki korak pred kriptografi.

Ponovimo

- ☞ Pri zamenjevalni šifri zamenjamo vrstni red črk v abecedi, pri premešanki pa zamenjamo vrstni red črk našega besedila.
- ☞ Frekvenčna analiza kot orodje uporablja pogostost črk. Z njo lahko razbijemo zamenjevalno šifro, če je le šifrirano besedilo dovolj dolgo. Pri odšifriranju nam pomagajo lastnosti posameznega jezika.
- ☞ Pri zamenjevalni šifri ni nujno, da črka zamenja črko, lahko jo tudi nek simbol, kot na primer pri prostozidarski šifri.

Naloge

1. Odšifriraj spodnji besedili. **Pomoč:** Eno besedilo je šifrirano z zamenjevalno šifro, drugo pa z premešanko.
   - MRFGBOCČV
   - ŠVIPARELO
2. Sestavi zamenjalne šifre s ključem:
   - TELEVIZIJA
   - ABECEDA
   - KRIPTOGRAFIJA
3. Z Atbashem odšifriraj:
   - AOCLNŠJNŠ
   - LNČZŠBŠJ
4. Kako se imenuje statistični postopek za razbijanje šifer, ki temelji na preverjanju pogostosti posamezne črke v besedilu?
5. S prostozidarsko šifro šifriraj besede
   - KRIPTOGRAF
   - KEY (to je ključ)
   - ANANAS
6. Po zgledu prostozidarske šifre sestavi kakšno svojo.

4 Vigenèrjeva šifra

Gospod Vigener je v 16.stol. razvil šifro, ki je dobila vzdevek "chiffre indechiffrable - šifra, ki je ni moč razbiti", saj je skoraj dve stoletji ni uspelo nikomur razvozlati. Šifra uporablja več abeced, kar pomeni, da se ista črka ne zamenja več vedno z isto črko, kot je bilo to v navadi pri zamenjevalnih šifrah.

Vigenèr

Blaise de Vigenère (April 5, 1523 - 1596) je bil francoski diplomat in kriptograf. Po njem je imenovana šifra, za katero so mnogi verjeli, da je ni moč razbiti.

Postopek šifriranja je podoben šifriranju Cezarjeve šifre. Le da pri šifriranju Vigenerjeve šifre izmenično uporabljamo več abeced.

1. Za lažje šifriranje, si najprej zapišemo Vigenerjev kvadrat. V prvi vrstici kvadrata je originalna abeceda, vsako vrstico nižje pa je zapisana abeceda, ki je za 1 premaknjena v levo zgornja abeceda.

original	**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**
menjava 1	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
menjava 2	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
menjava 3	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
menjava 4	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
menjava 5	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
menjava 6	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
menjava 7	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
menjava 8	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
menjava 9	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
menjava 10	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
menjava 11	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
menjava 12	L	M	N	O	P	R	S	Š	T	U		Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
menjava 13	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
menjava 14	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
menjava 15	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
menjava 16	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
menjava 17	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
menjava 18	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
menjava 19	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
menjava 20	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
menjava 21	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
menjava 22	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
menjava 23	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
menjava 24	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

2. Nato si izberemo ključno besedo, ki bo naš ključ za šifriranje, npr. KOVANEC. In z njim šifriramo besedilo: "Danes je lep dan." .

3. To naredimo tako, da prečrtamo vrstico, ki se začne na K (menjava 11), in stolpec, ki je označen z **d** v originalni abecedi. Črka, ki se nahaja na križišču črt, nam pove, da se d preslika v O.

4. Postopek ponovimo za naslednjo črko našega ključa in naslednjo črko besedila, torej, prečrtamo vrstico, ki se začne na O (menjava 15) in stolpec označen z **a**, na križišču pa spet izvemo, da se a preslika v O.

5. Enako storimo za vse ostale črke ključa in besedila. Opomba: Če je ključ krajši od besedila, ga ponovimo, ko nam ga zmanjka. Tako za črko e, iz besede "je", ponovno uporabimo vrstico, ki se začne na K (menjava 11) in stolpec e, in za l iz besede "lep", ponovno uporabimo vrstico, ki se začne na O (menjava 15) in stolpec l.

6. Če bi postopek ponavljali za celotno besedilo, bi dobili kriptogram: OOKEG OG ZTM DNŠ.

☞Ključna črka gesla, nam torej pove vrstico, besedilo pa stopec, ki ju moramo prečrtati. Križišče pa nam pove črko v katero se preslika željena črka.

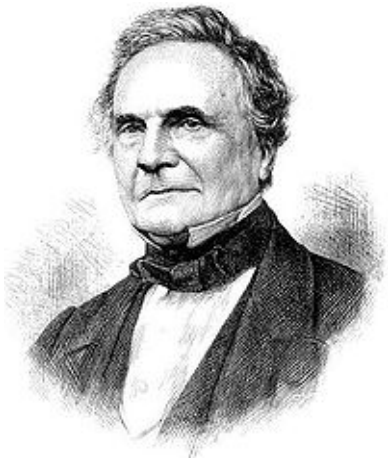
Odšifriranje poteka podobno:

1. Poznati moramo ključno besedo (KOVANEC). Če jo poznamo, pogledamo v vrstico, ki se začne na začetno črko ključne besede, (K (menjava 11)), v tej vrstici poiščemo prvo črko iz kriptograma (O) in pogledamo v prvo vrstico Vigenerjevega kvadrata, katera črka je originalna. S tem ugotovimo, da se je v O preslikal d.
2. Če postopek ponavimo še za preostale črke, dobimo nazaj originalno besedilo: "Danes je lep dan.".

Razbitje Vigenèrjeve šifre

Na žalost kriptografov in na srečo kriptoanalitkov je C. Babbagge uspešno razbil Vigenerjevo šifro. V kriptogramu je iskal dele besedil, ki so se ponavljali, ter jih je zapisal v tabelo. Zraven vsakega takega dela besedila, si je zapisal tudi, po koliko črkah se ponovijo in tudi vse deljitelje tega števila. Število, ki je skupno večini ponavljajočih se delov, predstavljala morebitno dolžino ključa.

Charles Babbage



Charles Babbage (26. december 1792 - 18. oktober 1871) je bil angleški matematik, filozof in praračunalnikar, ukvarjal se je s konstrukcijo stroja za računanje.

✎ Poiskusimo odšifrirati tole besedilo:

AOOLŠIPUTGUIVRCOGEKTNVŠLBZRKOTGOLEMKJCRDOGŽŽOLZRFK
PLRŠZPTSKOJZSPCVRŠPGZHFJŠUŠPEZLŠPGZHCBDSŽBLAKDNPUŽE
PFTTTCKAŽSGDFSSINLBDLTFNKAGCSGJLPLLLATČZTHEBCRHSHOI
JŠBŠPEBUŠPŠEIHNDBEBPJOTVEŠKDOGCERRAENUTNEAJNCETDFEŽ
ZACNZUZUHHIŽEADTJMNRCBLAKNRCNDVSŠSKAMCBŠSGKČCSEBTFŽ
REČTVČŽMUŽZMTHLPDLNPŠVLZZMBMFOAŠRTDNEGZRHŽBEBNRHSHO
FJMZŽOOGNŠPHGEDCEVOOPJZVTČLJDŠRFGFDNZGATZOEVGŠCVDZR
CTDMUŽZMTHLOSUŠZŽŠRNACHEIKEELPLRRŠŠZFBSKDOGCGCSITST
CMRNLJTICOSCŠSTIOKHLBZFŠDNPDTTAETFTCTAEBLDBFACUCVBV
KHŠCATORŠHCVTNJŠFKZLLLAŠGCGCVZIGAHCJŠZSBJVKČNNBPIAG
APPDLGŠNPCOBEBCNBDCCKVGZTGUVJIZOONDOGIORUBNNTDOEETI
AOIVUTAOŠLMNZKUTŠOBPSČŽMRNCKZRSLDNPDŽNEAJNFŽMUŽZMTH
LPFJSKČCTČNAKČCNNOČBCGEŽJFKVNECIŠGVVMZŠPKABECSCAAMA
CJVATMUŽZMPŽKVFLGZACCJRRAONACJVPGLDHJNOOIERZVČOKPJO
TVŽMAGTROJVKFEVJŽŠEBNNPFLIČSKČDLŽZCNUTKJŠZCUAFHČNČT
CLVŠHTFGVHSEČTAFHHJMOOGPFJIKDGABCRZB

1. Najprej moramo ugotoviti dolžino ključa. To storimo tako, da v šifriranem besedilu iščemo ponovitve zaporedja črk. Smiselno je iskati le ponovitve dolge vsaj 4 črke. Za vsk niz črk, si zapišemo tudi število po koliko črkah se je ponovil, ter delitelje te številke.

niz črk	ponovitev čez	deljitelji: 2	3	7	8	11	13	14	19	22
BLAK	133			x					x	
DOGC	217		x							
HSHO	154	x		x		x		x		x
KDOGC	217			x						
MTHL	98	x		x				x		
MUŽZMTHL	98	x			x		x			
PGZH	14	x		x				x		
RHSHO	154	x		x		x		x		x
ŠPGZH	14	x		x				x		
UŽZMTHL	98	x		x				x		
ZMTHL	98	x		x				x		
ŽZMTHL	98	x		x				x		

2. Nato pogledamo, kateri delitelj se največkrat pojavi. Ugotovimo, da je to število 7 in zato sklepamo, da ima ključ Vigenerjeve šifre dolžino 7.

3. Sedaj razdelimo zašifrirano besedilo v 7 skupin:

   - V prvo skupino damo 1., 8., 15., ... črko (črke na $7n + 1$ mestu, n =naravno število ali nič).
   - V drugo skupino damo 2., 9., 16., ... črko (črke na $7n + 2$ mestu, n =naravno število ali nič).
   - V tretjo skupino damo 3., 10., 17., ... črko (črke na $7n + 3$ mestu, n =naravno število ali nič).
   - V četrto skupino damo 4., 11., 18., ... črko (črke na $7n + 4$ mestu, n =naravno število ali nič).
   - V peto skupino damo 5., 12., 19., ... črko (črke na $7n + 5$ mestu, n =naravno število).
   - V šesto skupino damo 6., 13., 20., ... črko (črke na $7n + 6$ mestu, n =naravno število).
   - V sedmo skupino damo 7., 14., 21., ... črko (črke na $7n$ mestu, n =naravno število).

4. In vsako od teh besedil lahko enostavno odšifriramo, tako da uporabimo pogostost črk in postopek, imenovan frekvenčna analiza, ki smo ga opisali v 5. poglavju.

Če smo pri uporabi frekvenčne analize uspešni, ko vstavimo še presledke in ločila v besedilo, lahko za nagrado preberemo še drugi del zgodbice:

Naslednje jutro pa je volk dobil idejo, za katero je mislil, da bo resnično uspela. Rekel si je: »Preoblekel se bom v ovčko in jih prosil naj me spustijo notri.« In res se je volk oblekel v ovčko ter odšel pred hišico od pujskov.
Ko je potrkal je rekel: » Pozdravljeni pujski, jaz sem mala ovčka. Lačna sem in zebe me, "A me spustite notri?« Pujski so pogledali skozi okno in res so videli ovčko. Rekli so si: »Res je ovčka, spustimo jo notri, da se ne bo prehladila.« In pujski so odprli vrata. Volk pa je v trenutku, ko je prestopil prag hiše odvrgel ovčjo hišo in se zapodil za pujski. Ampak kakšna nesreča. Ker je bil volk nepreviden se je spotaknil ob lastne noge in padel v lonec vrele juhe. Glasno je zatulil in se pognal v gozd.
Doma si je volk pripravil culo in si rekel: »Ti pujski so prepametni zame, najbolje je da grem drugam in najdem manj pametne pujske.« In vrgel je culo na rame ter odšel daleč stran. Pujski pa so od takrat živeli lepo in mirno življenje, saj jih ni bilo več strah, da bi jih še kdaj preganjal volk.

Če postopek računamo na roke, je dolgotrajen. Vendar danes računalniki zmorejo še veliko več kot to. Ob določenih pogojih pa je to šifro res nemogoče razvozlati. To se zgodi takrat, ko je ključ tako dolg, kolikor je dolgo celotno besedilo. Izbran pa mora biti naključno, in ga smemo uporabiti le enkrat. Če se držimo teh pogojev, potem te šifre res ni moč razbiti.

Ponovimo

- ☞ Vigenèrjeve šifre skoraj dve stoletji ni uspelo nikomur razvozlati.
- ☞ Pri šifriranju Vigenèrjeve šifre izmenično uporabljamo več abeced.
- ☞ V 19.stoletju jo je razvozlal C. Babbagge.

✎ Naloge

1. Zašifriraj z Vigenèrjevo šifro in ključem SANJE:
   - Za dežjem vedno posije sonce.
   - Kdor drugemu jamo koplje, sam vanjo pade.
   - Na Gregorjevo se ptički ženijo.

5 Zgodba o Kraljici Mariji Stuart

Marija se je rodila kralju Jakobu V. leta 1542, vendar očeta nikoli ni spoznala. Le teden po Marijinem rojstvu, v starosti 30 let, je kralj Jakob V umrl. Ko je dopolnila komaj eno leto so jo kronali za kraljico. Angleži so želeli doseči spravo med deželama in so določili, da se mora Marija poročiti z Edvardom, angleškim princem. Vendar je škotsko sodišče določilo drugače. Marija se je tako morala poročiti s Francem, princem Francije. Ker sta bili tako Škotska kot Francija katoliški državi, naj bi njuna združitev pomenila večjo moč. Čeprav sta bila Franc in Marija takrat oba še otroka, je Francija obljubila Škotski pomoč ob morebitnih angleških napadih.

Kralj Jakob V. (1512-1542)

Angleži so po tem dogovoru povečali napade na Škotsko. Tudi ko je angleški kralj Henrik VIII. umrl, je njegov sin Edvard nadaljeval napade. Angleži so zmagovali, pustošili po Škotski, zato so Marijo v starosti 6 let poslali v Francijo. Tam je živela lepo, razkošno življenje, privzgojili so ji ljubezen do njenega bodočega ženina. Ko je bila Marija stara 16 let, sta se s Francem poročila. Po tem svečanem dogodku so pričakovali, da se bo Marija veličastno vrnila na Škotsko. Pa temu ni bilo tako. Franc je bil že kot otrok zelo slaboten in dovzeten za bolezni, nesrečno vnetje ušesa je bilo zanj usodno in že leto po poroki je umrl. Marija je bila stara komaj 17 let in že vdova. Njeno srečno otroštvo se je končalo.

Marija Stuart

Vrnila se je na škotsko in vnovič poročila, tokrat s bratrancem Henrikom Stuartom, lordom Darnleyjem. Rodila mu je sina, kljub temu pa je bil njun zakon nesrečen. Februarja leta 1567 so lord Darnleyja naši mrtvega, njo pa osumili umora.
V času ko kraljice ni bilo na škotskem, je protenstantizem na škotskih tleh vztrajno izpodrival katolištvo. Leta 1567 so škotski protestantje postali nezadovoljni s svojo katoliško kraljico. Zato so Marijo zaprli in jo prisilili, da se je odrekla kroni in jo prepustila sinu Jakobu VI, ki je bil takrat star le 14 mesecev. Cilj predaje krone je bil v tem, da je zastopstvo sina dobil Marijin polbrat lord Morayski (dokler Jakob ni dopolnil 18 let).

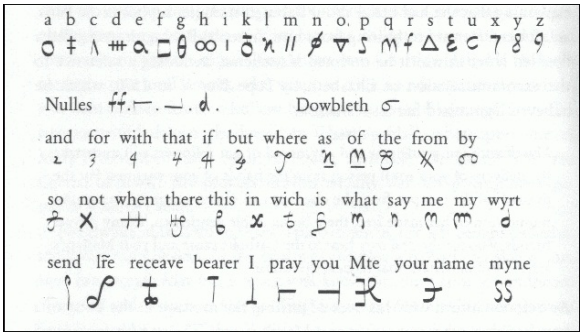
Čez eno leto je Marija pobegnila iz zapora in zbrala vojsko približno 6000 mož in z njimi še zadnjič poskušala osvojiti krono nazaj. Napad ji ni uspel. Razočarana Marija je zbežala v Anglijo in upala, da ji bo sestrična, kraljica Elizabeta I., nudila zatočišče. Vendar se je zmotila. Elizabeta je Mariji ponudila

le novo ujetništvo. Javni razlog za zaprtje je bila smrt Marijinega moža, lorda Darnleyja. Pravi razlog pa v tem, da je Marija predstavljala Elizabeti grožnjo, saj so imeli katoliški angleži katoličanko Marijo za svojo pravo kraljico, in ne protestantke Elizabete.

Marija ni imela pravice zahtevati krone, vendar katoliki Elizabete niso priznavali, saj je bila otrok iz drugega zakona kralja Henrika VII. Katoliki pa drugega zakona, zaradi ločitve, niso priznavali.
V Londonu je medtem nekaj katoliških angležev pripravljalo načrt, s katerim naj bi osvobodili kraljico Marija, usmrtili kraljico Elizabeto in organizirali upor. Zato so Mariji poslali zašifrirano pismo. Za šifriranje niso uporabljali enostavnega enoabecednega šifriranja ampak mešanico šifriranja črk in besed, uporabili pa so tudi prazne znake, znake brez pomena. Njihovo šifriranje je bilo sestavljeno iz 23 črk angleške abecede (manjkale so črke J, V in W) in 35. simbolov, ki so predstavljali besede ter 4 prazne znake. Posebej so imeli določen tudi znak, ki je pomenil, da se črka, ki stoji za njim podvoji.

Elizabeta I.

Za prenos teh pisem do Marije je na pomoč priskočil Gifford, kot je to počel že prej. Ker je bil Gifford duhovnik, ni bilo sumljivo, ko je venomer odhajal in prihajal. V tistem času pa je Anglija začela vršiti velik pritisk nad katoliki. Čeprav je bil Gifford Marijin sel že od začetka, je kljub temu igral dvojno igro. Vsa pisma, ki jih je nesel k Mariji ali pa od Marije odnesel, je vmes nesel tudi k njenim nasprotnikom, da so pisma prepisali. Pisma, ki so bila velikega pomena, so bila zašifrirana. Da bi nasprotniki razodeli vsebino pisma, so zaposlili Thomasa Pheliepesa, ki je bil izredno dober v razvozlavanju šifer. Šifrirni ključ Marijine šifre je našel že pred pismom, v katerem so Marijini privrženci izrazili željo po blagoslovu za upor.



del Marijinega nomenclatorja

Ko je Marija to prejela pismo, so nasprotniki samo še čakali, kdaj bo odgovorila. Marija je kmalu odgovorila, dala svoj blagoslov in s tem podpisala svojo smrtno obsodbo. Nasprotniki so tako imeli dovolj dokazov, da jo usmrtijo. A želeli so uničiti celotno zavezo, ki je načrtovala upor in usmrtitev kraljice Elizabete.
Zato je Pheliepes ponaredil pismo, v katerem je Marijo pozval naj izda imena vseh sodelujočih, pod pretvezo, da se bodo lahko zdaj, v zadnjih uricah pred uporom, lažje kontaktirali med sabo. Pismo so nato izročili Marija. Mary je pasti nasedla ter v odgovoru na pismo izdala imena vseh njenih zaveznikov.

Dokazov je bilo preveč, zato je kraljica Elizabeta ukazala usmrtiti kraljico Marijo in vse njene privržence. Kljub izmučenosti, je Marija na svojo usmrtitev prišla zravnano, ponosno. Njena zadnja misel pred giljotino je bila: "Moj konec je moj začetek.".

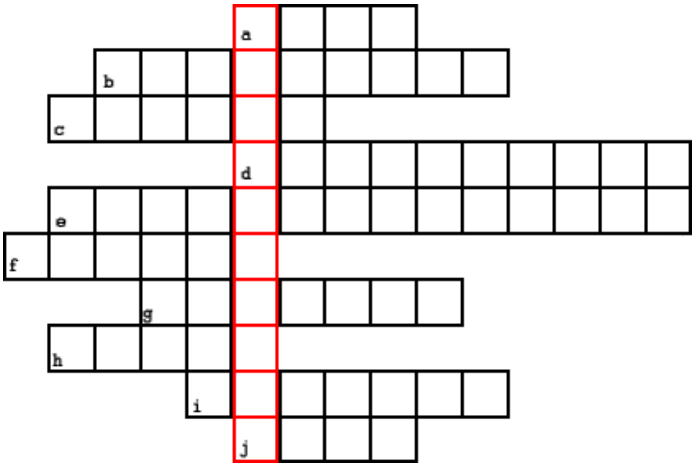
☞ Če ne bi uspeli odšifriratiMarijajine šifre, kraljica Elizabeta ne bi imela dokazov, da jeMarija sodelovala v zaroti proti njej in si je ne bi upala usmrtiti, saj bi s tem le še bolj tvegala, da se katoliki v državi uprejo. Maryjina usoda torej ni bila v njenih rokah, temveč v rokah kriptoanalitikov, kako hitro so lahko le-ti odšifrirali njena pisma. Thomas Phelipes pa bi imel težje delo, če bi za vsako pismo uporabili drug ključ za šifriranje.

Ponovimo

☞ Zelo pomembna je varnost šifer. Ker Marijaina šifra ni bila dovolj varna, je imela Elizabeta dokaz, da jo je lahko usmrtila.

Naloge

1. Križanka 1
   Navodilo: Rdeči kvadratki, brani od zgoraj navzdol, ti dajo rešitev križanke.
   (a) Šifra ali...
   (b) Z njim nekaj sporočamo.
   (c) Starogrški matematik.
   (d) Skrivni jezik.
   (e) Šifra zidarjev.
   (f) Skrivni jezik.
   (g) Po njem se imenuje »chifrre indechiffrable «
   (h) Rimski cesar.
   (i) S šifriranjem jo deloma dosežemo.
   (j) Zaradi razbitja šifre, ki jo je uporabljala, je bila obglavljena.



6 SLOVARČEK

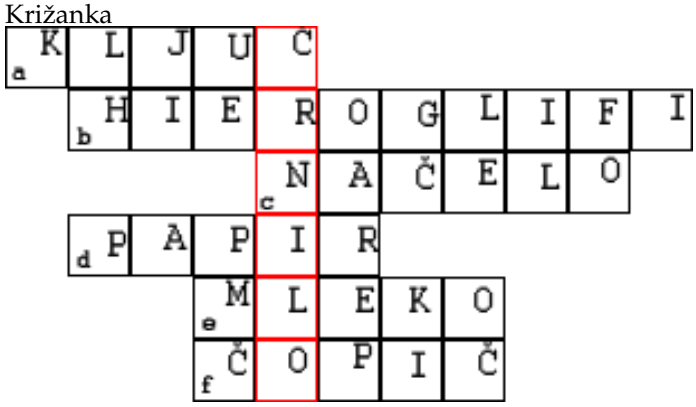
- **ALGORITEM** - postopek; navodila, kako nekaj izračunamo, naredimo
- **CEZARJEVA ŠIFRA** - enoabecedna šifra, ki za zamenjevalno abecedo uporablja abecedo, ki je za določeno število mest zamaknjena prvotna abeceda
- **ENOABECEDNA ŠIFRA** - šifra, ki uporablja eno abecedo za šifriranje, ista črka abecede se vedno preslika v isto črko **IZČRPNO ISKANJE** - tako imenujemo postopek iskanja, pri katerem pregledamo vse možne rešitve, na primer za primer razporejanja 6 črk, bi tako napisali vseh 720 možnih razporeditev in nato obkrožili vse smiselne besede. Obkrožene besede, nam nato predstavljajo rešitev izčrpnega iskanja.
- **KLJUČ** - beseda, geslo, ki ga uporabimo pri šifriranju,če ga poznamo, je razvozlanje šifre hitrejše
- **KERCKHOFFOVO NAČELO** - pravilo, ki pravi, da naš nasprotnik pozna način s katerim smo zašifrirali besedilo, ne pozna pa ključa, ki smo ga uporabili in vsa varnost našega kriptograma temelji na ključu
- **KODA** - šifra, pomeni dodelitev skrivnega pomena za besedo ali frazo.
- **KODER** - oseba, ki uporablja kode za skrivanje sporočil, kriptograf
- **KRIPTOANALITIK** - oseba, ki išče načine, kako prebrati skrito besedilo, če ne poznaš ključa, razbija šifre, kode
- **KRIPTOGRAF** - kriptograf je oseba, ki odkriva načine, kako skriti besedilo, da ga ne prebere neželjena oseba
- **KRIPTOGRAFIJA** - beseda je sestavljena iz dveh grških besed, KRIPTOS, ki pomeni skrito in GRAPHIA, ki pomeni pisati. Skupaj torej predstavljata skrito pisanje, je matematična veda, ki se ukvarja s skrivanjem in odkrivanjem skritih sporočil.
- **KRIPTOGRAM** - zašifrirano, skrito besedilo
- **PREMEŠANKA** - enoabecedna šifra, ki po nekem ključu premeša črke besedila, tako da nastane kriptogram
- **MODUL** - ostanek pri deljenju
- **NAPADALEC** - oseba, ki nam prisluškuje, želi pridobiti naše zaupne podakte ali pa jih celo spreminja, nam jih podtika ...
- **NOMENCLATOR** - je šifra, ki nekatere besede zamenja z drugimi besedami, nekatere črke pa z drugimi črklami. Je torej pol koda in pol šifra.
- **ODPRTO BESEDILO** - besedilu, ki ni zakljenjeno, šifrirano pravimo odprto ali pa tudi PROSTO besedilo
- **ODŠIFRIRANJE** - obratni postopek šifriranja, sporočilo v obliki, ki ni razumljiva vsakomur (kriptogram), preoblikuje v prvotno obliko, da ga lahko prebermo
- **PAPAJŠČINA** - skrivni jezik, za vsakim samoglasnikom dodamo p in samoglasnik ponovimo
- **ŠIFRA** - šifra je način skrivanja sporočila, kjer vsaki črki abecede posebej spremenimo pomen
- **PROSTO BESEDILO** - glej ODPRTO BESEDILO
- **TAJNOST** - pomeni ohranjanje skrivnosti, če je nekaj tajno, potem je skrito širši javnosti

- **VEČABECEDNA ŠIFRA** - šifra, ki uporablja več abeced, ena črka se ne preslika nujno vedno v isto črko (na primer: za dve abecedi, se sode črke spreminjajo po eni abecedi, lihe pa po drugi)
- **VIGENERJEVA ŠIFRA** - večabecedna šifra, ki namesto le ene zamenjevalne abecede, uporablja več le teh, kar ima za posledico to, da se lahko ista črka na različnih mestih v besedilu preslika v različne črke
- **ZAMENJALNA (SUBSTITUCIJSKA) ŠIFRA** - enoabecedna šifra v kateri originalno abecedo zamenjamo z neko drugo nadomestno (zamenjevalno) abecedo

7 REŠITVE

7.1 KLJUPUČ IPIN KLJUPUČAPANIPICAPA

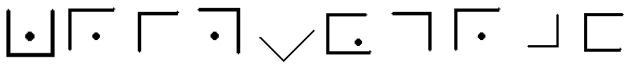
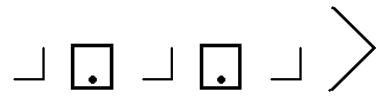
1. Kerckhoffovo načelo
2. - Matematika
   - Kriptogram
   - Cezar
3. Križanka



7.2 ZAMENJALNA ŠIFRA in PREMEŠANKA

1. - Algoritem
   - Praštevilo
2. Napisane so le menjalne abecede:

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

3. - Življenje
   - Ljubezen
4. Frekvenčna analiza.
5. - 
   - 
   - 

7.3 Vigenèrjeva šifra

1.
   - PASODČECGJVNDBTKIŽOZHNPO
   - DDDCIJUUOSNJNZTDOEVOZSNZCSNŽAUSDŠ
   - GAUCJAOFTJOOGOUMIRUNREČŠOH

7.4 Zgodba o Kraljici Mariji Stuart

1. Križanka