Del II
ZGODOVINA KRIPTOGRAFIJE

Tudi naši predniki so skrivali sporočila. S kriptografijo smo se ljudje spoznali že zelo zgodaj. Od nekdaj imamo potrebo po skrivnem prenašanju/hranjenju sporočil. V mnogih odločilnih bitkah v zgodovini je kriptografija odigrala pomembno vlogo.

Antična o obriti glavi na grškem delu

Genialni Histius je dal obriti sužnja in mu na glavo tetoviral sporočilo za Aristagorasa iz Grčije, naj začne upor. Nato je počakal, da so sužnju lasje zrasli, ter ga nato poslal v Grčijo z navodilom naj Aristagorasu reče: "*Obrijte mojo glavo in poglejte nanjo*." Nato je Aristagoras dvignil upor v Grčiji.

Histius je sporočilo za Aristagorasa le prikril. Kdor ni vedel, kje iskati sporočilo ga tudi ni mogel prebrati. Danes samo skrivanje sporočil ne predstavlja prevelike varnosti. Ko je sporočilo enkrat odkrito, ga lahko prebere kdorkoli.

Sporočila lahko prikrijemo na primer na naslednje načine:

- ☞ uporabimo limonino črnilo,
- ☞ uporabimo črnilo iz fenolftaleina,
- ☞ uporabimo črnilo iz mleka,
- ☞ naredimo vodni znak.

Navodilih za izdelavo prikritih sporočil najdeš v poglavju o steganografiji.

Lahko bi se zgodilo, da bi sužnja na poti nekdo že prej obril, in sporočilo bi bilo razkrito, upor pa ne bi bil uspešen. Zato samo prikrivanje sporočil za tajnost ni dovolj.

Sporočila lahko zavarujemo na primer na naslednje načine:

- ☞ sporočilo damo v ovojnico in jo zapečatimo,
- ☞ sporočilo položimo v skrinjico in jo zaklenemo,
- ☞ uporabimo drugačno abecedo,
- ☞ uporabimo šifro.

Več o boljšem varovanju sporočil najdeš v naslednjih poglavjih.

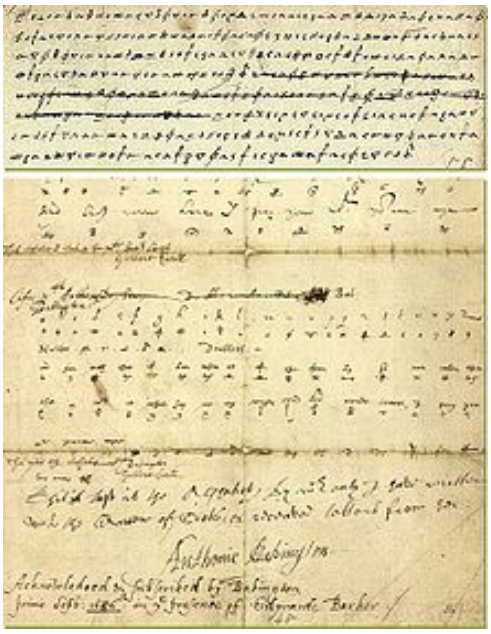
❀ **ŠIFRA - šifra je način skrivanja sporočila,**
kjer vsaki črki abecede posebej spremenimo pomen

Cezarjeva palica

Kako je Gaj Julij Cezar vedel ali je vojščak, ki mu je prinesel sporočilo, res njegov? Z vojščakom sta prelomila palico na pol, in vsak je vzel svojo polovico. Nato sta odšla na pot. Ko sta se ponovno srečala na bitki, sta staknila skupaj palici, in če sta se palici prilegali, sta vedela, da si lahko zaupata.

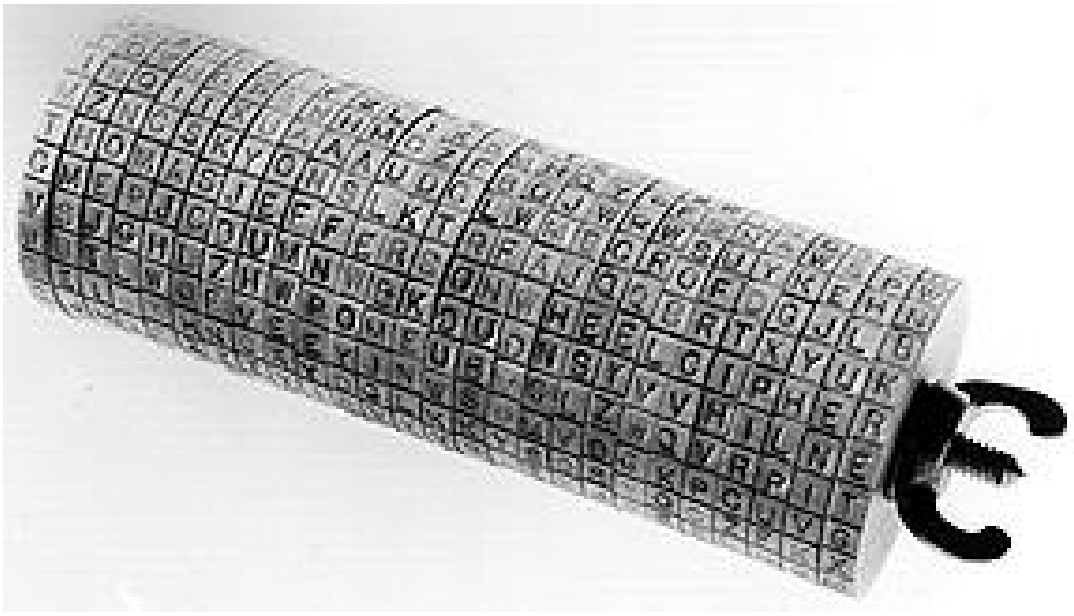
Srednji vek

V srednjem veku je kriptografijo največ uporabljala Cerkev. Papež Clement VII je naročil Gabrielu di Lavinda, da je ustvaril šifro imenovano "*nomenclator*". Le-ta se je uporabljala dobrih 450 let, kljub temu, da so bile vmes ustvarjene tudi varnejše šifre. Razlog temu je bila njena enostavnost.



☞Nomenclator je šifra, ki nekatere besede zamenja z drugimi besedami, nekatere črke pa z drugimi črklami. Nekatere take šifre še vse do danes niso razvozlane.

Leta 1518 je Johannes Trithemius napisal prvo tiskano knjigo o kriptografiji. Okoli 1790 je Thomas Jefferson s pomočjo matematika Dr. Roberta Pattersona izumil šifrarnik s kolesom. Le-tega so kasneje, v nekoliko drugačni obliku uporabljali med II. svetovno vojno v ameriški mornarici.



☞ Jeffersonovo kolo je sestavljeno iz 26 lesenih valjev (za vsako črko angleške abecede) z luknjo v sredini, v kateri je železna os. Valji se lahko neodvisno drug od drugega vrtijo okoli železne osi. Da z njim šifriramo besedilo, ga moramo razdeliti na sporočilca dolžine 26 črk. Vsako tako sporočilce nato posebej šifriramo. Na primer sporočilo iz slike: "$THOMASJEFFERSONWHEELCHIPER$" bi se šifriralo v "$VSJGHLZHWPOMEUBVSLZWQVRPIT$".

Po kratkem uvodu, bomo govorili o zamenjalnih šifrah, npr. o šifri, v kateri premešamo črke odprtega besedila medseboj. Opisan bo tudi postopek imenovan frekvenčna analiza, s katerim lahko brez poznavanja ključa iz kriptograma ugotovimo morebitno odprto besedilo.

Ključ in ključavnica

Sčasoma so ugotovili, da samo skrivanje besedil ni dovolj, saj 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.

Kot smo že omenili, se dajo tudi skrivni jeziki uporabiti za šifriranje. Če ne veš, v katerem jeziku je sporočilo napisano, ga ne moreš prebrati. Ko pa odkriješ za kateri skrivni jezik gre in se ga naučiš (oz. narediš slovar), besedilo hitro razvozljaš. Ključ je v tem primeru namig za kateri jezik gre in 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
- ☞ 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 je možnosti, 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 oziroma 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

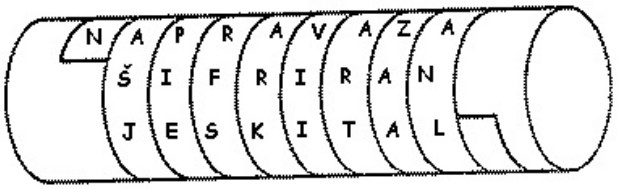
Skital je ena prvih naprav za šifriranje besedila. Uporabljali so ga že v Šparti okoli leta 475 p. n. št. Pošiljatelj in prejemnik sta imela palico v obliki valja z enakim polmerom. Pošiljatelj je okoli palice navil trak iz pergamenta in nanj po dolžini napisal sporočilo. Nato je trak odvil in ga poslal 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 zamenjalni 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

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: mškvpcpcnkvkm. 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.

Matematika skrita 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 $\bar{\text{K}}$=12. Ker želimo imeti črko K na prvem mestu abecede, moramo originalno besedo zavrteti za 11 mest (za ključ $\underline{\text{A}}$ ne zavrtimo abecede, za ključ $\underline{\text{B}}$ jo zvrtimo za 1 črko, za ključ $\underline{\text{C}}$ 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

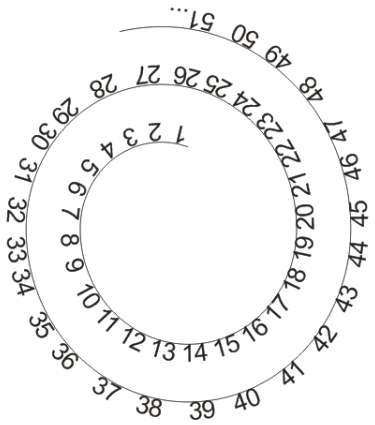
   ☞Opazimo, da nekatere številke nimajo pripadajočih črk. Natančneje, števila večja od 25 nimajo pripadajočih črk.

   ☞ 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”.

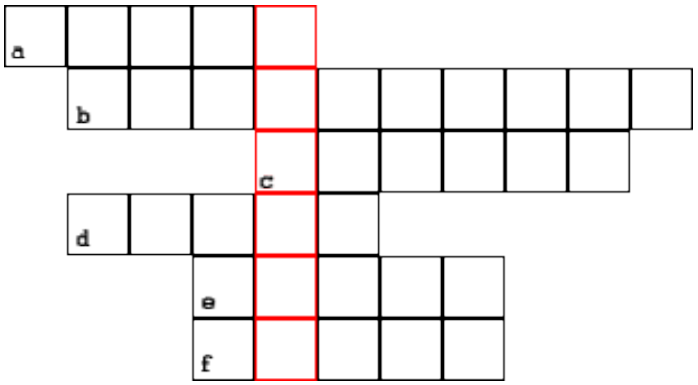
Ponovimo

- ☞ Včasih so pomembna sporočila le prikrivali, kar pa ni bilo najbolj varno. Kdor je vedel kje je sporočilo skrito, ga je lahko prebral. Lahko pa je tudi kdo po naključju odkril sporočilo.
- ☞ **KERCKHOFFOVO NAČELO** pravi, da varnost kriptograma ne sme biti odvisna od načina šifriranja, saj le tega nasprotnik (sčasoma s)pozna, pač pa mora varnost temeljiti na šifrirnem KLJUČU, 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.
- ☞ **ŠIFRIRANJE** - postopek preoblikovanja sporočila s pomočjo šifre v obliko, ki ni razumljiva vsakomur, obratni postopek imenujemo ODŠIFRIRANJE.
- ☞ **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).
- ☞ **ODPRTO BESEDILO** - besedilu, ki ni zakljenjeno/šifrirano, pravimo odprto ali pa tudi PROSTO besedilo.
- ☞ **KRIPTOANALITIK** - razbijalec šifer.
- ☞ S pomočjo znanih besedil so jezikoslovci razvozlali mnoge izumrle jezike in pisave. Najbolj znan primer so hieroglifi.

Naloge

1. Kakšno načelo se je razvilo skupaj z razvojem kripotgrafije?
2. Razbij Cezarjevo šifro: (a) ŽKFPŽKFTVK (b) VČTCFBSČKŽ (c) 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...



4. Naštej nekaj načinov kako lahko prikrijemo sporočilo?
5. Naštej nekaj načinov kako lahko zavarujemo sporočilo?

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 u, I v z,..., K v d.

✎ Z dano menjalno abecedo šifrirajmo sporočilo: “ZAMENJALNA ŠIFRA.”

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

✎ Z isto abecedo odšifrirajmo sporočilo: CMPSMMAČTČKM.

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

  originamedskip 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.

Ključ take šifre je kar cela menjalna abeceda. Uporabljena menjalna abeceda ima popolnoma naključen vrstni red črk. Slabost takšnega pristopa je, da si morata pošiljatelj in prejemnik oba zapomniti ta vrstni red. Ponavadi pa se pošiljatelj in prejemnik raje kot za celotno menjalno abecedo, dogovorita le za ključno besedo, ki določa vrstni red črk v menjalni abecedi. Poglejmo si primer.

✎ Recimo, da je naša ključna 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																								
menjava																								

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. V tem primeru je menjalna 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 zamenjalne šifre moramo ugotoviti vlogo črk v menjani abecedi. Da bi razbili zamenjalno 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.

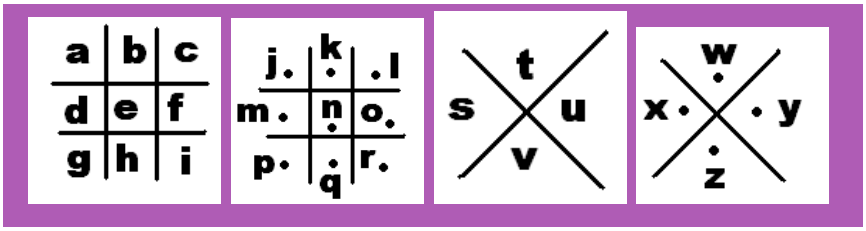
❀ **IZČRPNO ISKANJE** - tako imenujemo postopek iskanja, pri katerem pregledamo vse možne rešitve, za dani primer, bi tako napisali vseh 720 možnih razporeditev teh 6 črk in nato obkrožili vse smiselne besede. Obkrožene besede, nam nato predstavljajo rešitev izčrpnega iskanja.

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

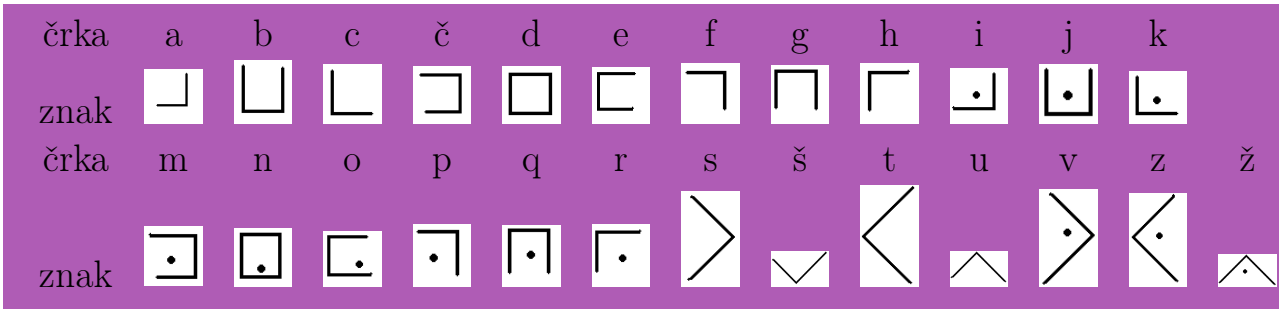
Zato raje začnemo iskanje s manjšimi ključi, in upamo, da kmalu najdemo ustrezno rešitev.

Prostozidarska šifra

Poglej si še naslednjo šifro:



To je posebna vrsta zamenjalne 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 zamenjalno 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.

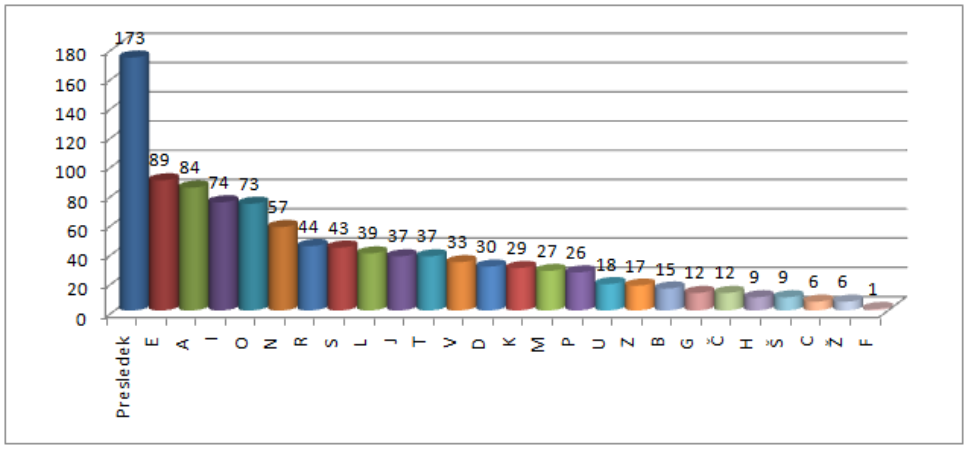
Uporaba frekvenčne analize

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

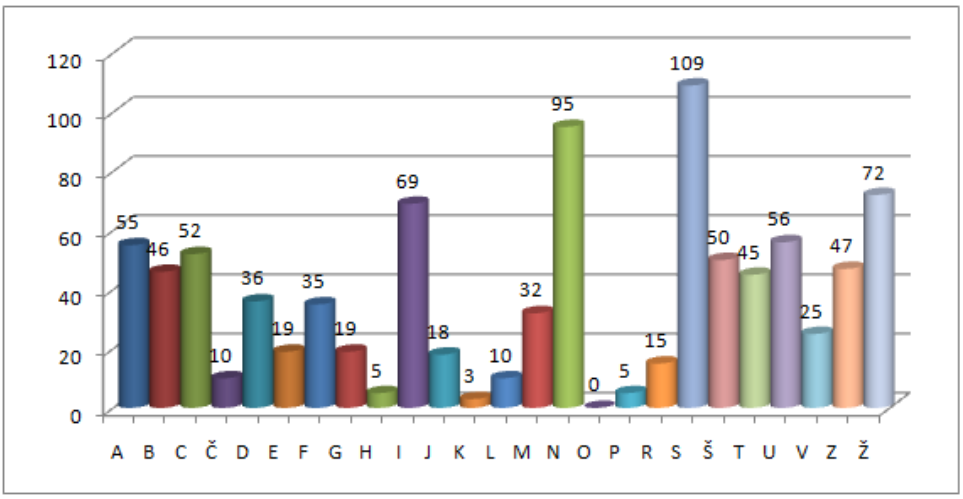
```
ZNTŽL ŠNHSF NUFŽU TTSCS ŠNZNG ZIZCT ŽHNUN UABSA BIFSD SANLN
ZTŽSG DBNRA EŠCTŽ FTSCŽ HSFNU SFRSČ SKSCB NMSPŽ GMIFC ITMIZ
ŠNABN VSČUŠ NFIUT ITŽJS ŠSRAB NDNZD IUMIJ SŠSRU IRTŽE ŠNUZI
ŠABNŠ ŠNAŽC TECSU CAUNG IDSCT ŽGSMS VZSTS ZŠSRA BNCNZ NDSDS
IVAIT FCNUN ZSČUŽ DITŽT ŽDCSŠ NABNM CDIFU ŠIUTŽ ŠNFŽU TUNGN
UCTŽG SMSVZ STŠNG ICUSČ IUŽMG ZŽDBI ŠAŽTI ZŠNVS CUSUŠ NMIŠN
ABSAE ŠCTSR ZIŽJS CTEUŽ FNKGI DŽŠNR SDBŽG JNHIU MŽVŽF FNZMI
BAICŽ AEŠCT SCIVŽ TŽCDI ZŠANT USMBE PSMIZ AICSŠ NFŽUT BNTNU
VŽPŽL NJSVS AIECA NUŽLN JSŠSR AŽCTE CSUAB NABSL IDSMI CNVAB
SŠIGN ZFŽUT AŽDNV JSVNC AECDS USFRS ČŽSZŠ IGJSŠ SREŠN USZBN
CŠNFŽ UTČNU MŽRSČ SKNŽM AEŠCT ŽFAŽD BTIUŠ NSZBN TNUMŽ JNBMI
ZAEŠC TSŠIG CNVFŽ UTŽMU ŽLSUC NVCNM IJŽVA BSŠIG NZSZB IMJSJ
SUFIČ ABSŠI DNUŠI VSŽMA BNDNF BIDIF NZMIB AICNA EŠCTS ZSCŽA
ECDSU SABND NZDID SZNFN BŠIVN VŽDSD SCSRE MŽJNZ FŽUTL NJSDS
ŽMABU SJSZI CGPBI JSUSZ SGZIC ABSAB IFSUA NLNZT ŽAŽŠM SMŽVŽ
FZNJŽ VŽDSŽ MABUS FNZMI BAICN FŽUTZ SAECD SUŽMP ZIDSS ZŠSRŠ
NČNZI ABNŠA BNABS LNFIU IVAIT ŠIGCN VBNCA BSŠIG NZFŽU TSZBN
CRŽLN VJSDS FIČAB SŠIDN UŠDŽM IAEŠC TSZSC ŽAŽAE CDSUS SZFŽU
TCNŠN VŽBIU AŽBIH NZFBZ SDSMŽ VŽF
```

1. Najprej moramo ugotoviti pogostost črk za jezik, v katerem je besedilo napisano.

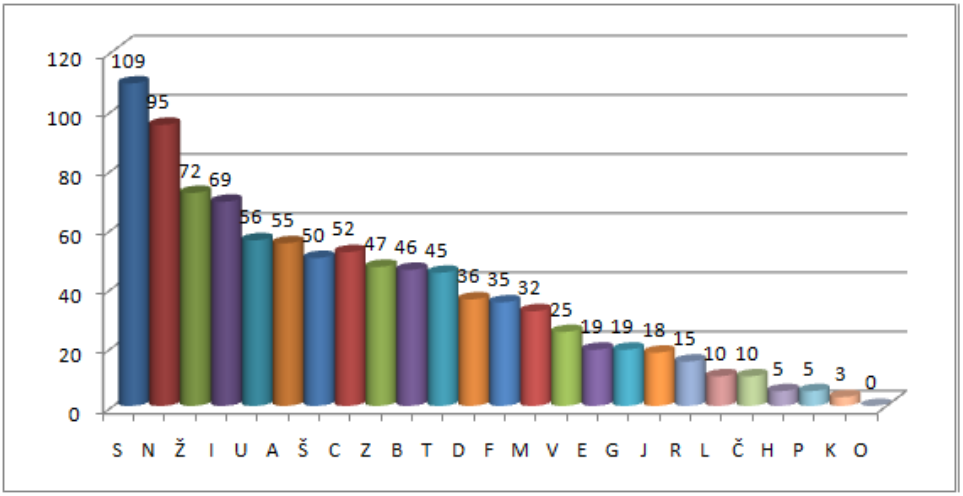
2. Besedilo je napisano v slovenščini. Na grafu je prikazana pogostost črk v slovenščini:



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:

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

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

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

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 zamenjalnih šifer je bila predvsem ta, da se ista črka vedno preslika v isto črko zamenjalne abecede. Zdelo se je, kot da so kriptoanalitiki korak pred kriptografi.

Ponovimo

- ☞ Pri zamenjalni 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 zamenjalno šifro, če je le šifrirano besedilo dovolj dolgo. Pri odšifriranju nam pomagajo lastnosti posameznega jezika.
- ☞ Pri zamenjalni 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 zamenjalno 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.