

Krüptoloogia I

(MTAT.07.002, 4 AP)

Loengud: T 12:15 aud. 405

Praktikumid: N 8:15 aud. 402

koduleht:

http://www.ut.ee/~peeter_l/teaching/kryptoi05s

(sisaldab loengumaterjale)

Hinde saamiseks: kaks kontrolltööd (järeltööd sessi ajal)

Funktsionaalsus: Süsteemi omadus teha neid asju, mida me tahame, et ta teeks.

Turvalisus: Süsteemi omadus mitte teha neid asju, mida me tahame, et ta ei teeks.

- (käideldavust arvestamata)

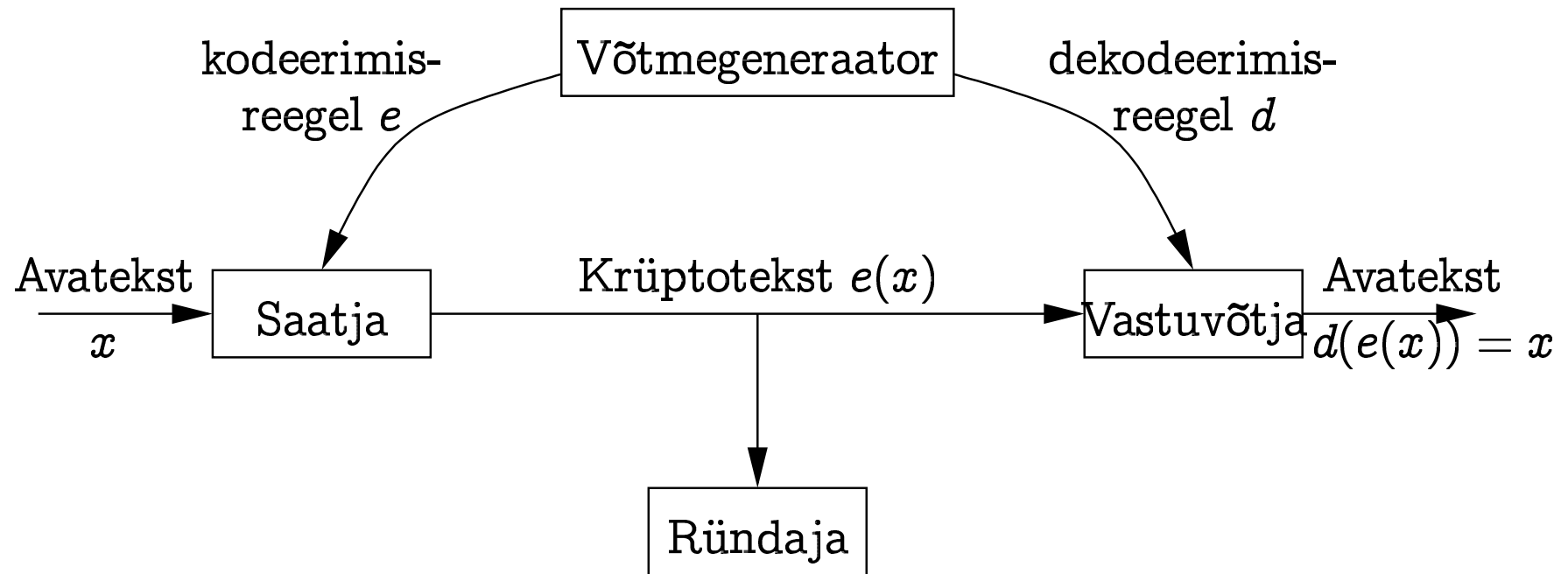
Krüptograafia: Matemaatilised meetodid süsteemi turvalisuse tagamiseks.

Krüptoanalüüs: Matemaatilised meetodid krüptograafia murdmiseks.

Krüptoloogia: Krüptograafia ja krüptoanalüüs koos.

Käesoleva kursuse materjalikästilus on rohkem laiuti kui sügavuti.

Šifreerimine ja dešifreerimine:

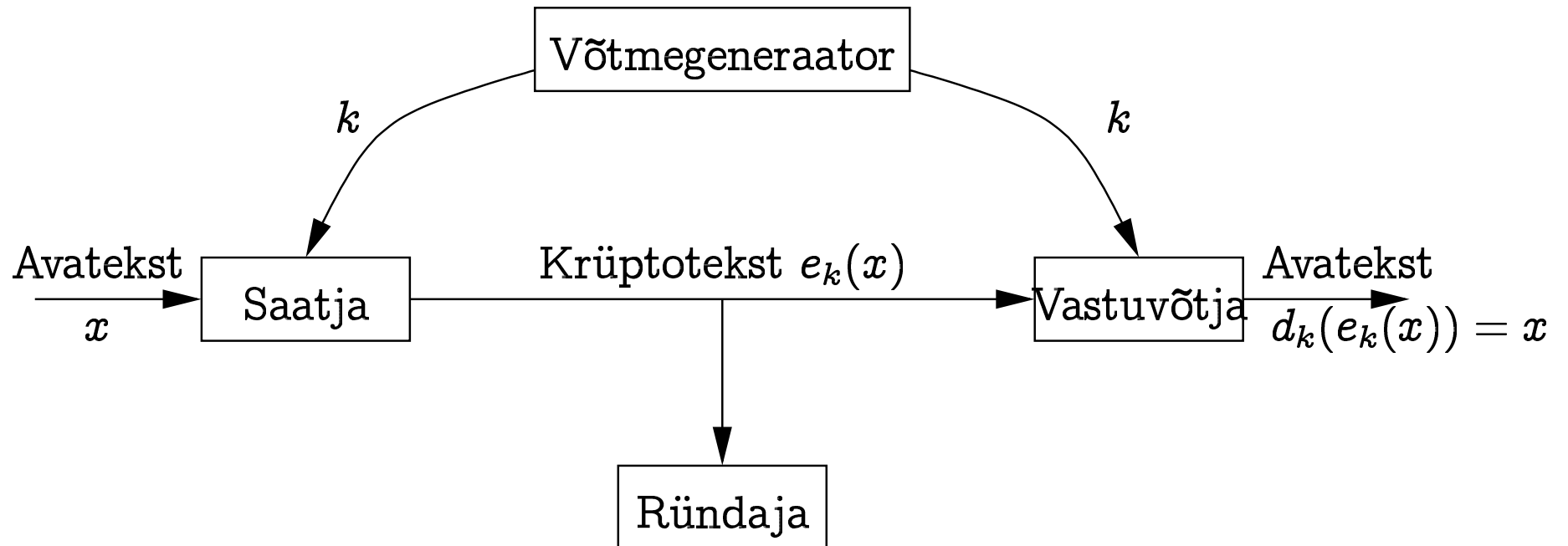


kodeerimis- ja dekodeerimisreegel peaksid olema lühidalt kirjeldatavad.

Krüptosüsteem on viisik $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, kus

- $\mathcal{P}$ on kõigi võimalike avatekstide hulk;
 - Sageli Σ^* mingi sobiva tähestiku Σ jaoks.
- $\mathcal{C}$ on kõigi võimalike krüptotekstide hulk;
- $\mathcal{K}$ on kõigi võimalike võtmete hulk;
- $\mathcal{E}$ on kodeerimis- ning $\mathcal{D}$ dekodeerimisreeglite hulk.
 - Kui $e \in \mathcal{E}$, siis $e : \mathcal{P} \longrightarrow \mathcal{C}$.
 - Kui $d \in \mathcal{D}$, siis $d : \mathcal{C} \longrightarrow \mathcal{P}$.
- Iga $k \in \mathcal{K}$ jaoks leiduvad $e_k \in \mathcal{E}$ ja $d_k \in \mathcal{D}$, nii et $d_k \circ e_k$ on samasusteisendus $\mathcal{P}$ -l.

Šifreerimine ja dešifreerimine:



kodeerimis- ja dekodeerimisreeglit kirjeldab k .

Vanad kreeklased, eriti spartalased, kasutasid krüptosüsteemina vahendit nimega $\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$ (*skytale*; pulk).



Dešifreerimiseks oli tarvis sama jämedusega pulka. Võti — pulga jämedus.

Kui teksti pikkus ei jagu täpselt ühele ringile mahtuvate tähtede arvuga, siis lisame lõppu mõttetud tähti.

Krüptoanalüüs: võtmeruumi täielik läbivaatus.

Ülesanne: murra lahti järgmine (ingliskeelne) *skytale*ga šifreeritud tekst (tühikute asemel on _):

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 2:

Fhartolr__ed_eonr_bh_ta_ec__ihflwem_otwttlhaesrr__
lGn__nn_lyfpehnwtrrar__aeldefi_uad_tsufmyaea_solkw
sni_oasatnh_eeleb_usnuueazosrceax_igadyv

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 3:

F_rele___dnsbmtees_kfneooathhesb_sGu_z_rfahiw daraa
od_idaot_f_a___lhsw__swnleeerulu_ansyee_xarvh_tlr
eue_ruhyaacoiwlimattt_alr__nnenolcpxngty

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 4:

Fatl_e_orb_ae_ifwmowther_ln_nlfenwrr_edf_a_sfye_ok
siosthelbunuaorexiayhror_den_ht_c_hle_ttlasr_G_n_y
phxta_aleiudtumaaslwn_aan_ee_suezsca_gdv

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 5:

F_oeeanu_eclfi_ates_lunsfxxdrri__etby_siseawhae_n_
zlehgrhalfddrfta_kl_otleruGenrp_wy_td_uoshaeohnmst
_eb_u_oyanaaaeri__ma__wwotnhlrsna_ceitv

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 6:

Frl__nbte_feoths_G__fhwaradiatfa_ls_sneeuuase_avht
reerhacilmttar_nnlpnt_ee_dsmesknoahebsuzraidao_do_
__hw_wlerl_nyexr_lfu_uyaowiat_l_neocxgy

Krüptotekst:

Frh_a_rateolldre_f_ie_du_aedo_ntrs_ubfhm_ytaae_ae_
cs_o_likhwfslnwie_mo_aostawttnthl_heaeelserbr__u_s
lnGunu_e_anzno_slrycfepaexh_nixgwatdryav

Dekodeerimine *skytalega* diameetriga 7:

Far_out_in_the_uncharted_backwaters_of_the_unfashi
onable_end_of_the_western_spiral_arm_of_the_Galaxy
_lies_a_small_unregarded_yellow_sunzyxwv

Skytale on näide ümberpaigutusšifrist.

Tähed jäävad samaks, järjekord muutub.

Järgmine näide on asendusšifrist.

Tähed jäävad sama koha peale, aga muutuvad millekski muuks.

Jäägiklassiring $\mathbb{Z}_n$:

- elemendid $\{0, 1, \dots, n - 1\}$;
- liitmine ja korrutamine: nagu $\mathbb{Z}$ -s, kuid *modulo* n .

Samastame ladina tähestiku ja ringi $\mathbb{Z}_{26}$: $A \equiv 0$, $B \equiv 1$, $\dots$, $Z \equiv 25$.

Nihkešiffer:

- $\mathcal{K} = \mathbb{Z}_{26}$.
- e_k : asendame iga tähe x kodeeritavas tekstis tähega $x + k$.
- d_k : asendame iga tähe x dekodeeritavas tekstis tähega $x - k$.

Tuntud ka kui Caesari šiffer.

ROT13 on nihkešiffer võtmega 13.

Näide:

- avatekst: „Quidquid latine dictum sit, altum viditur“

- võti: 5

x	ABC	DEF	GHI	JKL	MNO	PQR	STU	VWX	YZ
$e_5(x)$	FGH	IKJ	LMN	OPQ	RST	UVW	XYZ	ABC	DE

- krüptotekst „Vznivzni qfynsj inhyzr xny, fqyzr aninyzw“

Krüptoanalüüs: võtmeruumi täielik läbivaatus.

Ülesanne: murra lahti järgmine ingliskeelne nihkešifriga šifreeritud tekst:

Obr gc hvs dfcpzsa fsaowbsr; zchg ct hvs dscdzs ksfs asob,
obr acgh ct hvsa ksfs awgsfopzs, sjsb hvs cbsg kwhv
rwuwhoz kohqvsg.

Ülesanne: murra lahti järgmine ingliskeelne nihkešifriga šifreeritud tekst:

Obr gc hvs dfcpzsa fsaowbsr; zchg ct hvs dscdzs ksfs asob,
obr acgh ct hvsa ksfs awgsfopzs, sjsb hvs cbsg kwhv
rwuwhoz kohqvsg.

26 võtme läbiproovimine pole keeruline, aga...

Ülesanne: murra lahti järgmine ingliskeelne nihkešifriga šifreeritud tekst:

Obr gc hvs dfcpzsa fsaowbsr; zchg ct hvs dscdzs ksfs asob,
obr acgh ct hvsa ksfs awgsfopzs, sjsb hvs cbsg kwhv
rwuwhoz kohqvsg.

26 võtme läbiproovimine pole keeruline, aga...

Krüptotekstis esineb mitmel korral sõna „hvs“.

Ülesanne: murra lahti järgmine ingliskeelne nihkešifriga šifreeritud tekst:

Obr gc hvs dfcpzsa fsaowbsr; zchg ct hvs dscdzs ksfs asob,
obr acgh ct hvsa ksfs awgsfopzs, sjsb hvs cbsg kwhv
rwuwhoz kohqvsg.

26 võtme läbiproovimine pole keeruline, aga...

Krüptotekstis esineb mitmel korral sõna „hvs“.

Kas sellele vastav avatekst võiks olla „the“?

$$\text{hvs} \equiv 7, 21, 18$$

$$\text{the} \equiv 19, 7, 4$$

$$e_k(x) = x + k, \text{ seega } k = e_k(x) - x.$$

$$7 - 19 = 21 - 7 = 18 - 4 = 14 \pmod{26}$$

Krüptotekst:

Obr gc hvs dfcpzsa fsaowbsr; zchg ct hvs dscdzs ksfs asob,
obr acgh ct hvsa ksfs awgsfopzs, sjsb hvs cbsg kwhv
rwuwhoz kohqvsg.

Dekodeeritud võtmega 14:

And so the problem remained; lots of the people were
mean, and most of them were miserable, even the ones
with digital watches.

Nihkešiffer on erijuht [asendusšifrist](#).

- Võti: tähestiku Σ mingi permutatsioon σ .
- e_σ : asendame iga tähe x kodeeritavas tekstis tähega $\sigma(x)$.
- d_σ : asendame iga tähe x dekodeeritavas tekstis tähega $\sigma^{-1}(x)$.

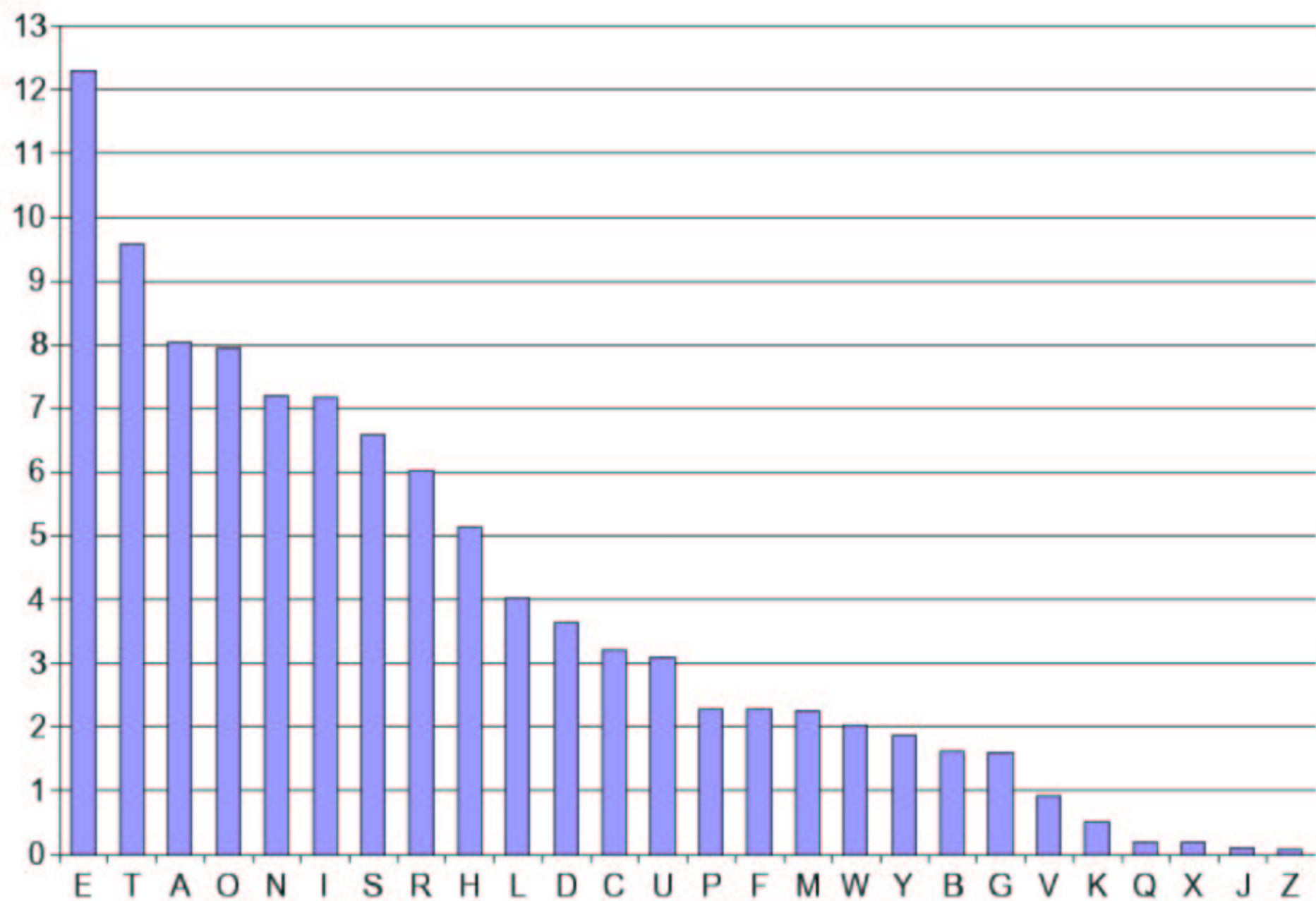
Krüptoanalüüs: võtmeid on $\geq 4 \cdot 10^{26}$, seega võtmeruumi ei saa läbi vaadata.

Murtav tähesagedusi analüüvides.

Tähesagedused inglise keeles (%):

<i>A</i>	8,05	<i>H</i>	5,14	<i>O</i>	7,94	<i>U</i>	3,10
<i>B</i>	1,62	<i>I</i>	7,18	<i>P</i>	2,29	<i>V</i>	0,93
<i>C</i>	3,20	<i>J</i>	0,10	<i>Q</i>	0,20	<i>W</i>	2,03
<i>D</i>	3,65	<i>K</i>	0,52	<i>R</i>	6,03	<i>X</i>	0,20
<i>E</i>	12,31	<i>L</i>	4,03	<i>S</i>	6,59	<i>Y</i>	1,88
<i>F</i>	2,28	<i>M</i>	2,25	<i>T</i>	9,59	<i>Z</i>	0,09
<i>G</i>	1,61	<i>N</i>	7,19				

Allikas: Jan Willemson, "Sissejuhatus krüptoloogiasse".



Sagedasemad tähepaarid:

<i>th</i>	1.52	<i>ha</i>	0.56	<i>is</i>	0.46	<i>se</i>	0.08
<i>he</i>	1.28	<i>es</i>	0.56	<i>or</i>	0.43	<i>le</i>	0.08
<i>in</i>	0.94	<i>st</i>	0.55	<i>ti</i>	0.34	<i>sa</i>	0.06
<i>er</i>	0.94	<i>en</i>	0.55	<i>as</i>	0.33	<i>si</i>	0.05
<i>an</i>	0.82	<i>ed</i>	0.53	<i>te</i>	0.27	<i>ar</i>	0.04
<i>re</i>	0.68	<i>to</i>	0.52	<i>et</i>	0.19	<i>ve</i>	0.04
<i>nd</i>	0.63	<i>it</i>	0.50	<i>ng</i>	0.18	<i>ra</i>	0.04
<i>at</i>	0.59	<i>ou</i>	0.50	<i>of</i>	0.16	<i>ld</i>	0.02
<i>on</i>	0.57	<i>ea</i>	0.47	<i>al</i>	0.09	<i>ur</i>	0.02
<i>nt</i>	0.56	<i>hi</i>	0.46	<i>de</i>	0.09		

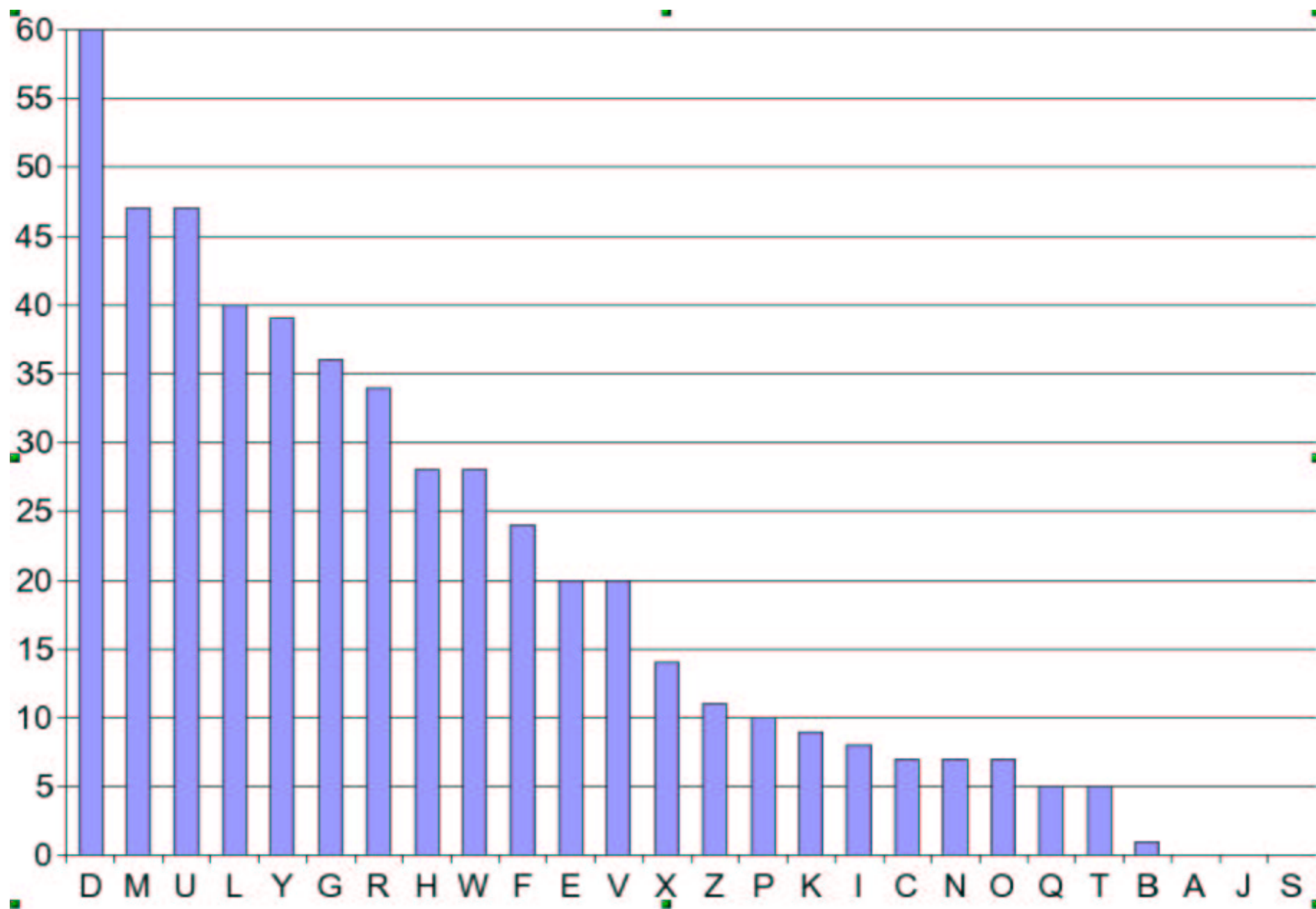
Sagedasemad tähekolmikud (kahanevalt): THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH.

Ülesanne: murra lahti järgmine ingliskeelne asendusšifriga šifreeritud tekst:

Myd lwez odhrlw ilh vylp myd ylxrd vur gw uwz vuz
rodngue vur Uhmyxh Fdwm, uwf myum vur lwez
kdnuxrd gm yuoodwdf ml kd myd lwd yd egcdf gw. Yd
yuf egcdf gw gm ilh uklxm myhdd zduhr, dcdh rgwnd yd
yuf plcdf lxm li Elwflw kdnuxrd gm pufd ygp wdhclxr
uwf ghhgmuked. Yd vur uklxm myghmz ur vdee, fuhq
yughdf uwf wcdh bxgmd um durd vgmy ygprdei. Myd
mygwt myum xrdf ml vlhhz ygp plrm vur myd iunm
myum odloed uevuzr xrdf ml urq ygp vyum yd vur
ellqgwt rl vlhhgdf uklxm. Yd vlhqdf gw elnue hufgl vygny
yd uevuzr xrdf ml mdee ygr ihgdwfr vur u elm plhd
gwmdhdrmgwt myuw mydz ohlkukez mylxtym. Gm vur,
mll - plrm li ygr ihgdwfr vlhqdf gw ufcdhmrgwt.

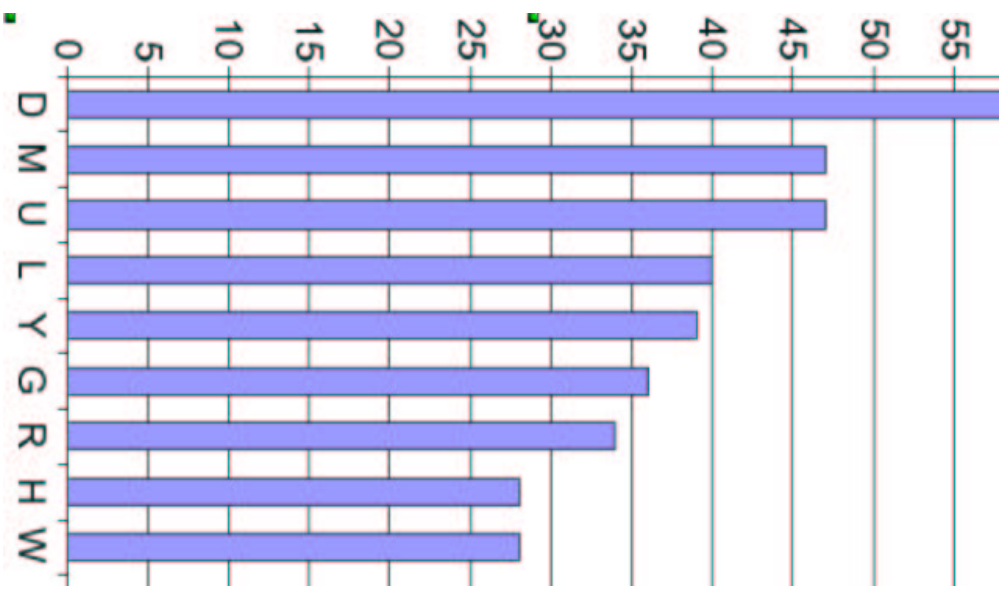
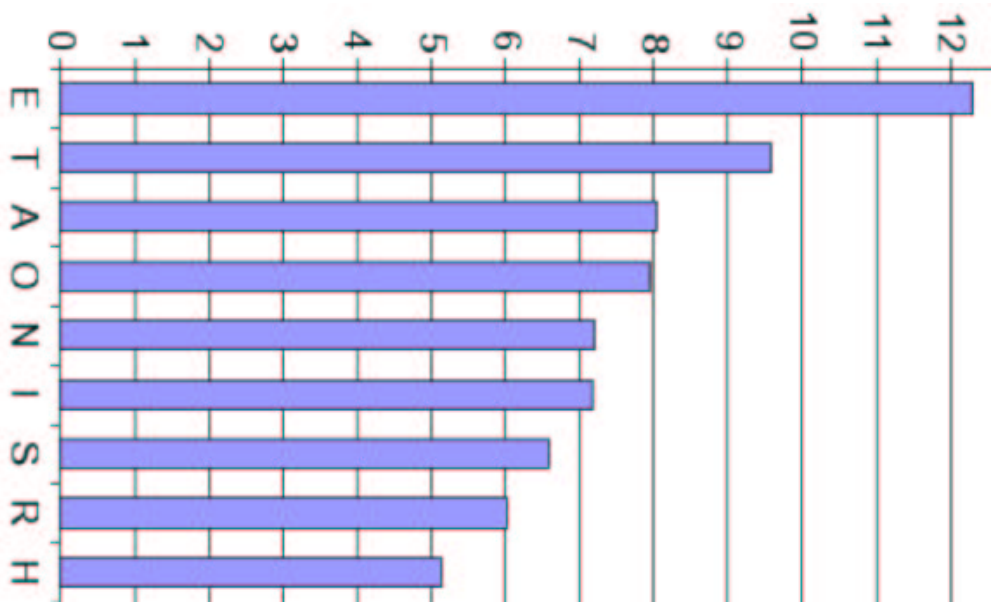
Esimene samm: loeme kokku, mitu korda mingi täht esi-
neb.

<i>a</i>	0	<i>h</i>	28	<i>o</i>	7	<i>u</i>	47
<i>b</i>	1	<i>i</i>	8	<i>p</i>	10	<i>v</i>	20
<i>c</i>	7	<i>j</i>	0	<i>q</i>	5	<i>w</i>	28
<i>d</i>	60	<i>k</i>	9	<i>r</i>	34	<i>x</i>	14
<i>e</i>	20	<i>l</i>	40	<i>s</i>	0	<i>y</i>	39
<i>f</i>	24	<i>m</i>	47	<i>t</i>	5	<i>z</i>	11
<i>g</i>	36	<i>n</i>	7				



d krüptotekstis on ilmselt e avatekstis.

Mye lwez oehrlw ilh vylp mye ylxre vur gw uwz vuz
roengue vur Uhmyxh Fewm, uwf myum vur lwez kenuxre
gm yuooewef ml ke mye lwe ye egcef gw. Ye yuf egcef gw
gm ilh uklxm myhee zeuhr, eceh rgwne ye yuf plcef lxm li
Elwflw kenuxre gm pufe ygp wehclxr uwf ghhgmukee. Ye
vur uklxm myghmz ur veee, fuhq yughef uwf weceh
bxgme um eure vgmy ygpreei. Mye mygwt myum xref ml
vlhhz ygp plrm vur mye iunm myum oeloe uevuzr xref
ml urq ygp vyum ye vur ellqgwt rl vlhhgef uklxm. Ye
vlhqef gw elnue hufgl vygny ye uevuzr xref ml meee ygr
ihgewfr vur u elm plhe gwmehermgwt myuw myez
ohlkukez mylxtym. Gm vur, mll - plrm li ygr ihgewfr
vlhqef gw ufcehmgrgwt.



Avateksti T — krüptoteksti M või U

Avateksti A ja O — krüptoteksti U/M, L, Y
jne.

Loeme kokku sagedasemad tähepaarid...

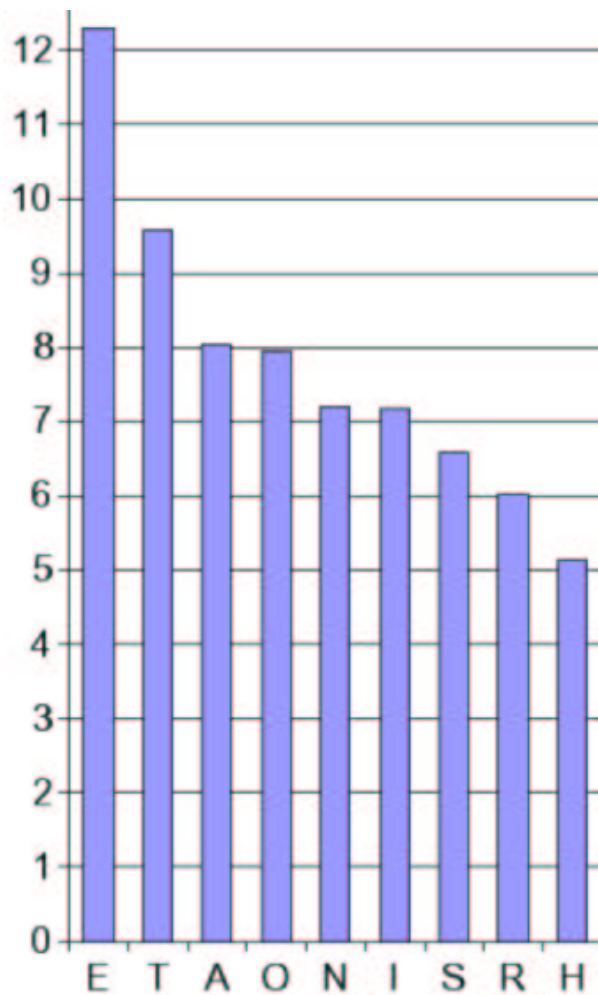
krüptotekst

avatekst

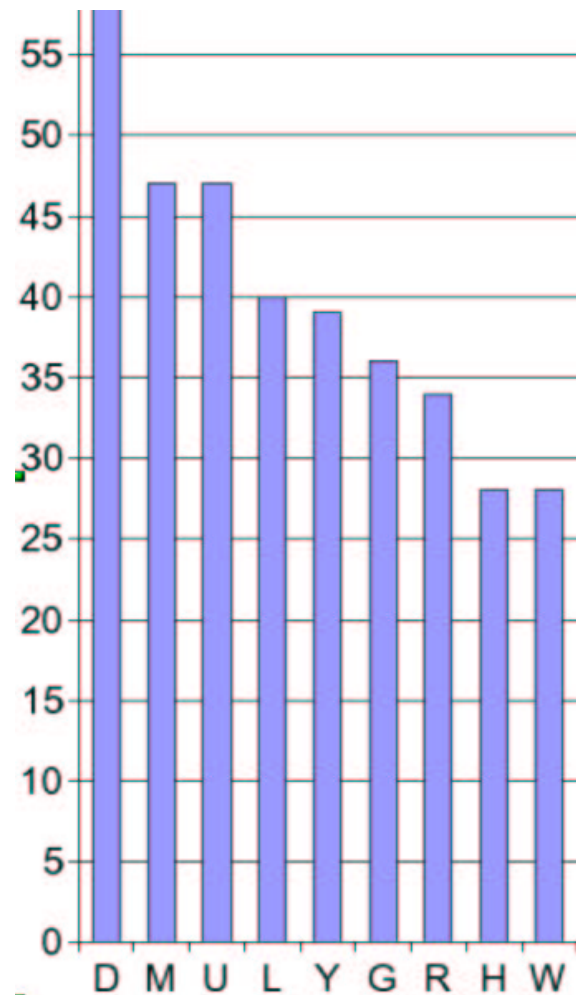
<i>my</i>	16	<i>yg</i>	9	<i>th</i>	1.52	<i>at</i>	0.59
<i>yd</i>	13	<i>yu</i>	9	<i>he</i>	1.28	<i>on</i>	0.57
<i>df</i>	11	<i>rd</i>	8	<i>in</i>	0.94	<i>nt</i>	0.56
<i>gw</i>	11	<i>gm</i>	7	<i>er</i>	0.94	<i>ha</i>	0.56
<i>ur</i>	11	<i>lh</i>	7	<i>an</i>	0.82	<i>es</i>	0.56
<i>vu</i>	11	<i>lx</i>	7	<i>re</i>	0.68	<i>st</i>	0.55
		<i>xr</i>	7	<i>nd</i>	0.63	<i>en</i>	0.55

m (krüpto) — t(ava). y(krüpto) — h(ava).

The lwez oehrlw ilh v~~h~~lp the hlxre vur gw uwz vuz
ro~~e~~ngue vur Uh~~t~~hxh Few~~t~~, uwf ~~t~~hut vur lwez kenuxre gt
huooewef ~~t~~l ke the lwe he egcef gw. He huf egcef gw gt ilh
uklxt ~~t~~hhee zeuhr, eceh rgwne he huf plcef lxt li Elwflw
kenuxre gt pufe hgp wehclxr uwf ghhgtukee. He vur uklxt
~~t~~hghtz ur vee, fuhq hughef uwf weceh bxgte ut eure vgth
hgpreei. The thgwt ~~t~~hut xref ~~t~~l vlhhz hgp plrt vur the
iunt ~~t~~hut oeloe uevuzr xref ~~t~~l urq hgp v~~h~~ut he vur
ellqgwt rl vlhhgef uklxt. He vlhqef gw elnue hufgl v~~h~~gnh
he uevuzr xref ~~t~~l teee hgr ihgewfr vur u elt plhe
gw~~t~~ehertgwt ~~t~~huw thez ohlkukez ~~t~~hlxt~~t~~. Gt vur, ~~t~~ll -
plrt li hgr ihgewfr vlhqef gw ufcehtgrgwt.



eht



dym

u(krüpto) on kas a või o(ava).

The lwez oehrlw ilh v~~h~~lp the hlxre vur gw uwz vuz
ro~~e~~ngue vur Uh~~th~~xh F~~e~~w~~t~~, uwf thut vur lwez kenuxre gt
huooewef tl ke the lwe he egcef gw. He huf egcef gw gt ilh
uklxt th~~h~~ee zeuhr, e~~c~~eh rgwne he huf plcef lxt li Elwflw
kenuxre gt pufe hgp wehclxr uwf gh~~h~~gtukee. He vur uklxt
th~~g~~htz ur v~~e~~ee, fuhq hughef uwf we~~c~~eh bxg~~t~~e ut eure vg~~th~~
hgpreei. The thgwt thut xref tl vlhhz hgp plrt vur the
iunt thut oeloe uevuzr xref tl urq hgp v~~h~~ut he vur
ellqgwt rl vlhhgef uklxt. He vlh~~q~~ef gw elnue hufgl v~~h~~gn~~h~~
he uevuzr xref tl tee hgr ihg~~e~~wfr vur u el~~t~~ plhe
gw~~t~~ehertgwt thuw thez ohlkukez thlx~~t~~ht. Gt vur, tll -
plrt li hgr ihg~~e~~wfr vlh~~q~~ef gw ufce~~h~~tgrgwt.
u(krüpto) on a(ava).

The lwez oehrlw ilh vhlp the hlxre var gw awz vaz
roengae var Ahthxh Fewt, awf that var lwez kenaxre gt
haoowef tl ke the lwe he egcef gw. He haf egcef gw gt ilh
aklxt thhee zeahr, eceh rgwne he haf plcef lxt li Elwflw
kenaxre gt pafe hgp wehclxr awf ghhgtakee. He var akuxt
thghtz ar veee, fahq haghef awf weceh bxgte at eare vgth
hgpreei. The thgwt that xref tl vlhhz hgp plrt var the
iant that oeloe aevazr xref tl arq hgp vhat he var
ellqgwt rl vlhhgef akuxt. He vlhqef gw elnae hafgl vhgnh
he aevazr xref tl teee hgr ihgewfr var a elt plhe
gwtehertgwt thaw thez ohlakez thlxtht. Gt var, tll - plrt
li hgr ihgewfr vlhqef gw afcehtgrgwt.

The lwez oehrlw ilh vhlp the hlhre var gw awz vaz
roengae var Ahthxh Fewt, awf that var lwez kenaxre gt
haooewef tl ke the lwe he egcef gw. He haf egcef gw gt ilh
aklxt thhee zeahr, eceh rgwne he haf plcef lxt li Elwflw
kenaxre gt pafe hgp wehclxr awf ghhgtakee. He var akuxt
thghtz ar vee, fahq haghef awf weceh bxgte at eare vgth
hgprei. The thgwt that xref tl vlhhz hgp plrt var the
iant that oeloe aevazr xref tl arq hgp vhat he var
ellqgwt rl vlhhgef akuxt. He vlhqef gw elnae hafgl vhgnh
he aevazr xref tl teee hgr ihgewfr var a elt plhe
gwtehertgwt thaw thez ohlkakez thlxtht. Gt var, tll - plrt
li hgr ihgewfr vlhqef gw afcehtgrgwt.

h(krüpto) on r(ava)

The lwez oerrlw ilr vhlp the hlhre var gw awz vaz
roengae var Arthxr Fewt, awf that var lwez kenaxre gt
haoewef tl ke the lwe he egcef gw. He haf egcef gw gt ilr
aklxt three zearr, ecer rgwne he haf plcef lxt li Elwflw
kenaxre gt pafe hgp werclxr awf grrgtakee. He var aklt
thgrtz ar veee, farq hagref awf wecer bxgte at eare vgth
hgprei. The thgwt that xref tl vlrrz hgp plrt var the iant
that oeloe aevazr xref tl arq hgp vhat he var ellqgwt rl
vlrrgef aklt. He vlrqef gw elnae rafgl vhgnh he aevazr
xref tl teee hgr irgewfr var a elt plre gwterertgwt thaw
thez orlkakez thlxtht. Gt var, tll - plrt li hgr irgewfr
vlrqef gw afcertgrgwt.

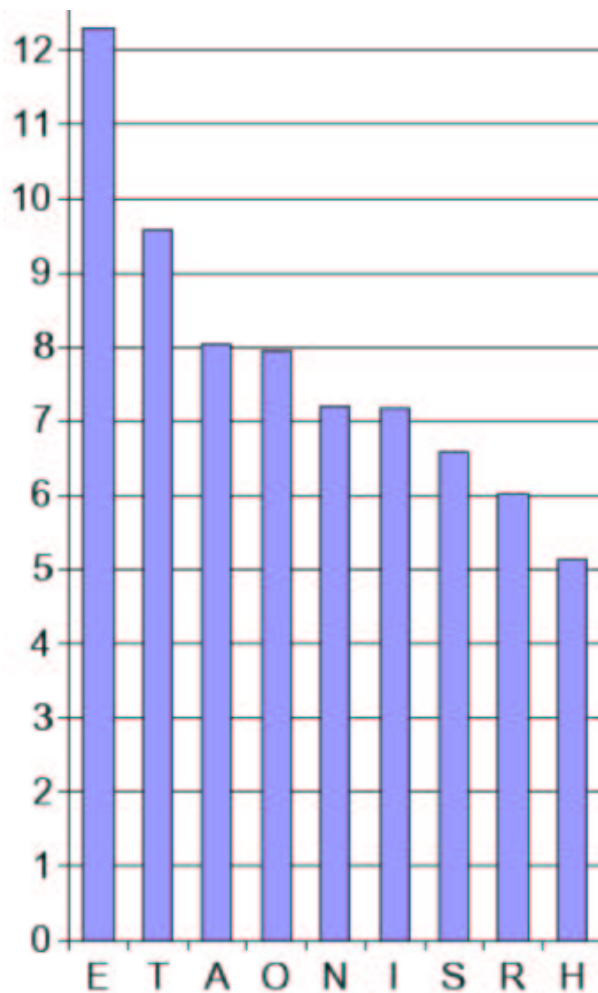
The lwez oerrlw ilr vhlp the hlhre var gw awz vaz
roengae var Arthxr Fewt, awf that var lwez kenaxre gt
haoowef tl ke the lwe he egcef gw. He haf egcef gw gt ilr
aklxt three zearr, ecer rgwne he haf plcef lxt li Elwflw
kenaxre gt pafe hgp werclxr awf grrgtakee. He var aklt
thgrtz ar vee, farq hagref awf wecer bxgte at eare vgth
hgprei. The thgwt that xref tl vlrrz hgp plrt var the iant
that oeloe aevazr xref tl arq hgp vhat he var ellqgwt rl
vlrrgef aklt. He vlrqef gw elnae rafgl vhgnh he aevazr
xref tl teee hgr irgewfr var a elt plre gwterertgwt thaw
thez orlkakez thlxtht. Gt var, tll - plrt li hgr irgewfr
vlrqef gw afcertgrgwt.

x(krüpto) on u(ava)

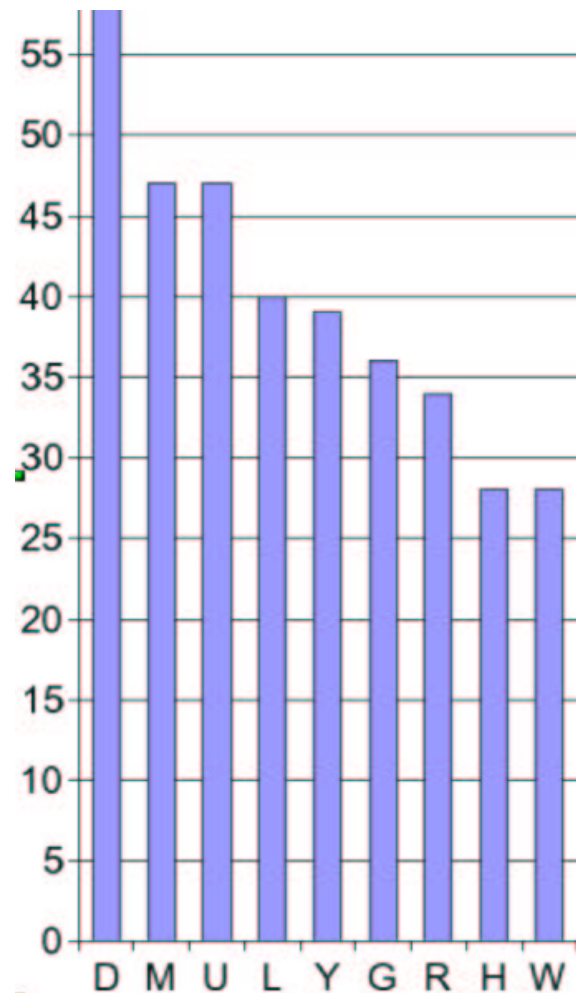
The lwez oerrlw ilr vhlp the hlure var gw awz vaz
roengae var Arthur Fewt, awf that var lwez kenaure gt
haoowef tl ke the lwe he egcef gw. He haf egcef gw gt ilr
aklut three zearr, ecer rgwne he haf plcef lut li Elwflw
kenaure gt pafe hgp werclur awf grrgtakee. He var aklut
thgrtz ar veee, farq hagref awf wecer bugte at eare vgth
hgpreei. The thgwt that uref tl vlrrz hgp plrt var the iant
that oeloe aevazr uref tl arq hgp vhat he var ellqgwt rl
vlrrgef aklut. He vlrqef gw elnae rafgl vhgnh he aevazr
uref tl teee hgr irgewfr var a elt plre gwterertgwt thaw
thez orlkakez thlutht. Gt var, tll - plrt li hgr irgewfr
vlrqef gw afcertgrgwt.

The lwez oerrlw ilr vhlp the hlure var gw awz vaz
roengae var Arthur Fewt, awf that var lwez kenaure gt
haoewef tl ke the lwe he egcef gw. He haf egcef gw gt ilr
aklut three zearr, ecer rgwne he haf plcef lut li Elwflw
kenaure gt pafe hgp werclur awf grrgtakee. He var aklut
thgrtz ar vee, farq hagref awf wecer bugte at eare vgth
hgprei. The thgwt that uref tl vlrrz hgp plrt var the iant
that oeloe aevazr uref tl arq hgp vhat he var ellqgwt rl
vlrrgef aklut. He vlrqef gw elnae rafgl vhgnh he aevazr
uref tl teee hgr irgewfr var a elt plre gwterertgwt thaw
thez orlkakez thlutht. Gt var, tll - plrt li hgr irgewfr
vlrqef gw afcertgrgwt.

g(krüpto) ja l(krüpto) on täishäälikud.



aehrthu



udyhmx

$g(\text{krüpto})$ ja $l(\text{krüpto})$ esinevad sagedasti, $y(\text{ava})$ ei esine.
 $g(\text{krüpto})$ on $i(\text{ava})$ ja $l(\text{krüpto})$ on $o(\text{ava})$.

The owez oerrow ior vhop the houre var iw awz vaz roeniae var Arthur Fewt, awf that var owez kenaure it haooewef to ke the owe he eicef iw. He haf eicef iw it ior akout three zearr, ecer riwne he haf pocef out oi Eowfow kenaure it pafe hip wercour awf irritakee. He var akout thirtz ar vee, farq hairef awf wecer buite at eare vith hipreei. The thiwt that uref to vorrz hip port var the iant that oeoee aevazr uref to arq hip vhat he var eooqiwt ro vorrief akout. He vorqef iw eonae rafio vhin he aevazr uref to tee hir iriewfr var a eot pore iwterertiwt thaw thez orokakez thoutht. It var, too - port oi hir iriewfr vorqef iw afcertiriwt.

The owez oerrow ior vhop the houre var iw awz vaz roeniae var Arthur Fewt, awf that var owez kenaure it haooewef to ke the owe he eicef iw. He haf eicef iw it ior akout three zearr, ecer riwne he haf pocef out oi Eowfow kenaure it pafe hip wercour awf irritakee. He var akout thirtz ar vee, farq hairef awf wecer buite at eare vith hipreei. The thiwt that uref to vorrz hip port var the iant that oeoee aevazr uref to arq hip what he var eooqiwt ro vorrief akout. He vorqef iw eonae rafio vhin he aevazr uref to tee hir iriewfr var a eot pore iwterertiwt thaw thez orokakez thoutht. It var, too - port oi hir iriewfr vorqef iw afcertiriwt.

r(krüpto) on s(ava). f(krüpto) on d(ava). b(krüpto) on q(ava). v(krüpto) on w(ava). w(krüpto) on n(ava).

The onez oerson ior whop the house was in anz was soeniae was Arthur Dent, and that was onez kenance it haooened to ke the one he eiced in. He had eiced in it ior akout three zears, ecer sinne he had poced out oi Eondon kenance it pade hip nercous and irritakee. He was akout thirtz as wee, darq haired and necer quite at ease with hipseei. The thint that used to worrz hip post was the iant that oeooee aewazs used to asq hip what he was eooqint so worried akout. He worqed in eonae radio whinh he aewazs used to tee his iriends was a eot pore interestint than thez orokakez thoutht. It was, too - post oi his iriends worqed in adcertisint.

Ja nüüd on juba lihtne...

The only person for whom the house was in any way special was Arthur Dent, and that was only because it happened to be the one he lived in. He had lived in it for about three years, ever since he had moved out of London because it made him nervous and irritable. He was about thirty as well, dark haired and never quite at ease with himself. The thing that used to worry him most was the fact that people always used to ask him what he was looking so worried about. He worked in local radio which he always used to tell his friends was a lot more interesting than they probably thought. It was, too - most of his friends worked in advertising.

x	abcdefghijklmnopqrstuvwxyz
$\sigma(x)$	uknfditygsqepwlobhrmxcvjza

Asendusšifri kõikvõimalikud kodeerimisreeglid moodustavad rühma.

Sama kehtib nihkešifri jaoks.

- Iga $k, k' \in \mathcal{K}$ jaoks leidub $k'' \in \mathcal{K}$ nii, et $e_{k'} \circ e_k = e_{k''}$.
 - Nihkešifril $k'' = k + k'$, asendusšifril $k'' = k' \circ k$.
- Leidub võti $k \in \mathcal{K}$, et e_k on samasusteisendus.
- Iga $k \in \mathcal{K}$ jaoks leidub $k' \in \mathcal{K}$ nii, et $e_k = d_{k'}$.

Asendusšiffer on **monoalfabeetiline**, s.t. iga täht šifreeritakse alati samaks täheks.

Näitena poliüalfabeetilisest šifrist vaatame **Vigenère'i šifrit**.

Põhimõtteliselt on tegemist erinevatele tekstipositsioonidele erineva võtmega nihkešifrite rakendamisega.

Näide: olgu meil võti „secret“ ja tekst „this has been hidden well“. Võti on siis (18, 4, 2, 17, 4, 19).

t	h	i	s	h	a	s	b	e	e	n
19	7	8	18	7	0	18	1	4	4	13
18	4	2	17	4	19	18	4	2	17	4
11	11	10	9	11	19	10	5	6	21	17
l	l	k	j	l	t	k	f	g	v	r
h	i	d	d	e	n	w	e	l	l	
7	8	3	3	4	13	22	4	11	11	
19	18	4	2	17	4	19	18	4	2	
0	0	7	5	21	17	15	22	15	13	
a	a	h	f	v	r	p	w	p	n	

Krüptotekst: „llkj ltk fgvr aahfvr pwpn“.

Ülesanne: murra lahti järgmine ingliskeelne Vigenère'i šifriga kodeeritud tekst:

We ywqzeq iddug bjt cnjkc bhb eduyl ute imtn lvbvae;
fbtpntm odnfbtduf ajpdbeu aobugs aal ntacmf ligp vwe
gqpn fyqezeeqpvy fyiot, bhb cal jiu fuvmv. We ozgptumf p
svtgct gpcck lww io gpg Seabtpsfsqu. Ihr Lgcteiuhif itt aa
cpguyg vgiom qu gbctbaalu, p wvtf qug xntafipi bhvew
wuwo ihr Dqvoaa jpd emetngta iaxmp io ruraolqpvy af
kcieeqpvy sgihu oa bjtie tqcg uiwa fymgis, bv vwe fbtxcg
cpseeavpnqqpvy tuiv ihrg mtec bjtmfmnkef dggy zcew tb
bjtmfmnkef.

Esimene samm: leiame võtme pikkuse.

Üks võimalus selle leidmiseks on [Kasiski test](#):

Otsime krüptotekstist identseid lõike pikkusega ≥ 3 . On tõenäoline, et need vastavad identsetele avatekstilõikudele. Nendevaheline kaugus jagub siis võtmepikkusega.

We ywqzeq iddug bjt cnjkc bhb eduyl ute imtn lvbvae;
fbtpntm odnfbtduf ajpdbeu aobugs aal ntacmf ligp vwe
gqpn fyqezeeqp v fyiot, bhb cal jiu fuvmv. We ozgptumf p
svtgct gpcck lww io gpg Seabtpsfqu. Ihr Lgcteiuhif itt aa
cpguyg vgiom qu gbctbaalu, p wvtf qug xntafipi bhvew
wuwo ihr Dqvoaa jpg emetngta iaxmp io ruraolqp v af
kcieeqp v sgi hu oa bjtie tqcg uiwa fymgis, bv vwe fbtxcg
cpseeavpnqqp v tuiv ihrg mtec bjtmfmnkef dggy zcew tb
bjtmfmnkef.

„bjtmfmnkef“-de vahekaugus on 20. „ajpd“-de vahekaugus
on 175. „bjt“-de vahekaugus on 265 ja 55. Võtmepikkus
on ilmselt 5.

Teine võimalus: [kokkulangevusindeks](#).

Teksti s kokkulangevusindeks $I_c(s)$ on tõenäosus, et kahel juhuslikult valitud positsioonil s -s asub sama täht.

$$\text{Olgu } p_{s,x} = \frac{x\text{-i esinemiste arv } s\text{-s}}{|s|}. \text{ Siis } I_c(s) = \sum_{x \in \Sigma} p_{s,x}^2 .$$

Juhusliku stringi s korral $I_c(s) \approx 0.038$ ($|\Sigma| = 26$).

Ingliskeelse teksti s korral $I_c(s) \approx 0.066$ (tõenäosused eespool toodud tabelist).

Monoalfabeetilise šifriga šifreeritud ingliskeelse teksti s korral samuti $I_c(s) \approx 0.066$.

Kui valime krüptotekstist välja positsioonid, kus on šifreerimisel kasutati sama nihet, peaks vastava osateksti I_c olema ≈ 0.066 .

Kui valime positsioonid, kus on kasutatud mitut erinevat nihet, siis näib tulemus juhuslikum ja tema I_c peaks olema väiksem.

Oletame et võtmepikkus on 1. Krüptoteksti I_c on ≈ 0.049 . Seega võib arvata, et seal on mitut erinevat nihet kasutatud ja oletus on vale.

Oletame, et $|k| = 2$. Siis s_{paaris} on

wyqeidgjcjcheultitlbaftnmdftuapbuousanamlgveqnyeeqvyobbajuumwogtmpv
gtpclwopsatsqirgtihftacgyvimubtalpvfuxtfpbvwohdvajdmtgaamirroqvfce
qvghobteqgiaygsvwftccsevnqvuvhgtcjmmkfgycwbjmmkf

ja s_{paaritu} on

ewzqdubtnkbbdyuemnvvebptonbdfjdeabgaltcfipwgpqzepfithclifvvezpufst
cgckwiggebpfuhlceuiitapuggoqgcbauwtqgnaiihewwirqoapeentixpoualpakie
psiuajitcuwfmibvebxgpeapqptiirmebtfnedgzetbtfne

Kokkulangevusindeksid on vastavalt 0.049 ja 0.056. Ilmselt liiga väiksed.

Oletame et $|k| = 3$. Siis s_0 on

wwedgtjbeytmlvfpmntfpeogatmivgnqepytbluvwztfvcpkwgsbsurciitag
giqbblwfgtibeuidojettaapraqaceviojecifgbwbcpepqtvrtdmnfgctjfk

s_1 on

eqqdbckhdletvabnofdadubslafgwqfeevibcjfmegupttclipetfiltuftcu
voucauvqxaphwhqapmnaxiuopfjqshattgwyivetgsanpuigejfkdyebtme

s_2 on

yziujncbuuinbettdbujbauanclepypyzqfohaiuvopmsggcwogapqhgehiapy
gmgtaptunfivworvadegimorlvkepgubiquamsvfxcevqvihmctmegzwbmnf

ja kokkulangevusindeksid on vastavalt 0.056, 0.052 ja 0.049.

$|k| = 4$ korral on kokkulangevusindeksid
0.054, 0.064, 0.053, 0.059.

$|k| = 5$ korral on kokkulangevusindeksid
0.081, 0.083, 0.082, 0.090, 0.076.

$|k| = 6$ korral on kokkulangevusindeksid
0.055, 0.069, 0.057, 0.065, 0.054, 0.059.

Nii et ilmselt $|k| = 5$. Kokkulangevusindeksite suurus on
tingitud teksti lühidusest.

Viis teksti, igaüks neist saadud nihkešifrit rakendades:

wzdtcdtnapddpastlwnzvtafwppccispichtggubpqtiiwivptiiavivutcaiwxspvittkgwtk
eeucbuelennudoaaiefefbluetstkoeshtiaufigawuabwhodnaooaesoigfsecenthemeytme
yqgnhyivftffbbacggyeyhjvouvglgafrefayobavgfhuraegxrlfegaeuybfgequrcfffzbf
wibjblmbbmbaeulmpqqqibimzmtwpbqliicgmcltxivwdamtmuqkqibtimvbcaqigbmdcbm
qdjkeutvtotjugnfvpepocuvfgfcwgtugutpvqtufnpeoqjeaprpcphjqwgvtppvpmjngejn

Olgu need tekstid $s_0, \dots, s_4$. Olgu võtme tähed $k_0, \dots, k_4$.

Kui s_i tähtedest lahutame k_i , siis saame midagi, kus tähed on jaotunud nagu ingliskeelses tekstis.

Järgmine samm: püüame leida $k_i - k_j$ erinevate i ja j jaoks.

Tekstide s ja s' vastastikune kokkulangevusindeks $MI_c(s, s')$ on tõenäosus, et s -i juhuslikul positsioonil olev täht langeb kokku s' -i juhuslikul positsioonil oleva tähega.

$$MI_c(s, s') = \sum_{x \in \Sigma} p_{s,x} p_{s',x}$$

Kui nii s kui ka s' on ingliskeelsed tekstid, siis $MI_c(s, s') \approx 0.066$.

$MI_c(s, s')$ ei muutu, kui rakendame s -le ja s' -le sama monoalfabeedilist šifrit (sama võtmega).

Olgu p_x tähe x esinemissagedus inglise keeles. Olgu s ingliskeelne tekst. Olgu s' saadud ingliskeelses tekstist rakendades talle nihkešifrit võtmega ℓ .

$$MI_c(s, s') = \sum_{i=0}^{25} p_i p_{i+\ell},$$

s.t. $MI_c(s, s')$ sõltub ainult ℓ -st.

Sama MI_c saaksime, kui s -le oleks rakendatud nihkešifrit võtmega i ja s' -le võtmega $i + \ell$.

Vastavad MI_c väärtused on (sõltuvalt ℓ -st):

0	0.066	7	0.038	14	0.039	20	0.036
1	0.040	8	0.033	15	0.045	21	0.033
2	0.032	9	0.035	16	0.038	22	0.044
3	0.033	10	0.038	17	0.035	23	0.033
4	0.044	11	0.045	18	0.033	24	0.032
5	0.033	12	0.039	19	0.038	25	0.040
6	0.036	13	0.043				

Seega suudame me ilmselt ära tunda, kui s -le ja s' -le on rakendatud nihkešifrit sama võtmega.

Meil olid $s_0, \dots, s_4$. Olgu s_i^ℓ saadud s_i -st, rakendades talle nihkešifrit võtmega ℓ .

Siis s_i^ℓ on saadud tekstist, kus tähed jaotuvad nagu inglise keeles, rakendades talle nihkešifrit võtmega $k_i + \ell$.

Iga i, j, ℓ jaoks uurime, kas s_i ja s_j^ℓ on saadud tekstidest, kus tähed jaotuvad nagu inglise keeles, rakendades neile nihkešifrit sama võtmega.

Kui jah, siis $k_i = k_j + \ell$.

$MI_c(s_0, s_1^\ell)$:

0	0.039	7	0.038	14	0.050	20	0.031
1	0.042	8	0.046	15	0.069	21	0.046
2	0.044	9	0.031	16	0.033	22	0.044
3	0.032	10	0.027	17	0.035	23	0.030
4	0.042	11	0.044	18	0.043	24	0.031
5	0.030	12	0.032	19	0.037	25	0.042
6	0.036	13	0.027				

Ilmselt siis $k_0 = k_1 + 15$.

$MI_c(s_0, s_2^\ell)$:

0	0.027	7	0.027	14	0.055	20	0.042
1	0.039	8	0.040	15	0.051	21	0.054
2	0.055	9	0.033	16	0.034	22	0.037
3	0.038	10	0.042	17	0.049	23	0.036
4	0.033	11	0.029	18	0.036	24	0.044
5	0.033	12	0.029	19	0.029	25	0.035
6	0.026	13	0.046				

Väärtuse $k_0 - k_2$ kohta ei julge midagi väga kindlat ütelda.
Tõenäolised on 2 või 14 või 21; ehk ka 15.

$MI_c(s_0, s_3^\ell)$:

0	0.049	7	0.074	14	0.049	20	0.045
1	0.027	8	0.027	15	0.029	21	0.035
2	0.032	9	0.034	16	0.030	22	0.041
3	0.048	10	0.041	17	0.040	23	0.027
4	0.030	11	0.039	18	0.058	24	0.029
5	0.029	12	0.030	19	0.034	25	0.044
6	0.037	13	0.041				

Ilmselt siis $k_0 = k_3 + 7$.

$MI_c(s_0, s_4^\ell)$:

0	0.052	7	0.039	14	0.038	20	0.038
1	0.035	8	0.028	15	0.045	21	0.030
2	0.044	9	0.039	16	0.032	22	0.034
3	0.035	10	0.037	17	0.036	23	0.028
4	0.045	11	0.030	18	0.026	24	0.038
5	0.033	12	0.036	19	0.041	25	0.047
6	0.053	13	0.062				

Võib arvata, et $k_0 = k_4 + 13$.

$MI_c(s_2, s_4^\ell)$:

0	0.044	7	0.032	14	0.031	20	0.028
1	0.042	8	0.030	15	0.045	21	0.033
2	0.038	9	0.033	16	0.045	22	0.042
3	0.028	10	0.045	17	0.048	23	0.030
4	0.031	11	0.068	18	0.044	24	0.034
5	0.040	12	0.056	19	0.029	25	0.039
6	0.030	13	0.036				

Ilmselt siis $k_2 = k_4 + 11$.

$$k_0 = k_1 + 15$$

$$k_0 = k_3 + 7$$

$$k_0 = k_4 + 13$$

$$k_2 = k_4 + 11$$

Võimalikeks võtmeteks on siis „zkxsm“ ja kõik temast nihkešifrit rakendades saadavad sõnad. Need on:

alytn, bmzuo, cnavp, dobwq, epcxr, fqdys, grezt, hsfau, itgbv, juhcw, kvidx, lwjey, mxkfz, nylga, ozmhb, panic, qbojd, rcpke, sdqlf, termg, ufsnh, vgtoi, whupj, xivqk, yjwrl

Proovime nad kõik järgi.

Võti „panic“ annab

He looked about the cabin but could see very little; strange monstrous shadows loomed and leaped with the tiny flickering flame, but all was quiet. He breathed a silent thank you to the Dentrassis. The Dentrassis are an unruly tribe of gourmands, a wild but pleasant bunch whom the Vogons had recently taken to employing as catering staff on their long haul fleets, on the strict understanding that they keep themselves very much to themselves.