

WSTĘP DO KRYPTOGRAFII

ĆWICZENIA I (klasyczne metody szyfrowania)

Zagadnienia:

- szyfr Cezara,
- szyfr Vigenere'a,
- szyfr Playfaira,
- kryptoanaliza szyfru Cezara.

Notacja i założenia:

- tekst tajny P ,
- alfabet tekstu tajnego:

$$\Sigma_P = \{a, \mathring{a}, b, c, \mathring{c}, \dots, x, y, z, \mathring{z}, \mathring{z}\} \cup \{\text{znak odstępu ' '}\}, |\Sigma_P| = 34,$$

- tekst jawny C ,
- alfabet tekstu jawnego:

$$\Sigma_C = \{A, \mathring{A}, B, C, \mathring{C}, \dots, X, Y, Z, \mathring{Z}, \mathring{Z}\} \cup \{\text{znak odstępu ' _'}\}, |\Sigma_C| = 34,$$

Szyfr Cezara - charakterystyka:

- szyfr podstawieniowy monoalfabetyczny,
- trzy podstawowe warianty tabeli podstawień:
 - przesunięcie alfabetu tekstu jawnego o $1 \leq k \leq |\Sigma_C|$ znaków,
 - użycie słowa kluczowego $\alpha \in \Sigma_C^*$ takiego, że
$$\forall i, j \in \{1, 2, \dots, |\alpha|\} : i \neq j \Rightarrow \alpha[i] \neq \alpha[j],$$
 - losowa permutacja alfabetu Σ_C .

Przesunięcie alfabetu o k znaków:

- niech np. $k = 5$, wtedy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
Y	Z	Ż	Ź	'_'	A	Ą	B	C	Ć	D	E	Ę	F	G	H	I
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
J	K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T	U	W	X

- tekst tajny $\mathbf{P} = \text{kryptografia} \mapsto \mathbf{C} = \text{FNŚMÓLĆNYCEY}$,
tekst jawny $\mathbf{C} = \text{ÓYĘĄIJEŻY} \mapsto \mathbf{P} = \text{tajemnica}$,
- kryptoanaliza wyczerpująca: $|\Sigma_{\mathbf{C}}|$ przypadków.

Użycie słowa kluczowego $\alpha \in \Sigma_C^*$:

- niech np. $\alpha = \text{CEZAR}'_'$, wtedy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
C	E	Z	A	R	_	Ą	B	Ć	D	Ę	F	G	H	I	J	K
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
L	Ł	M	N	Ń	O	Ó	P	S	Ś	T	U	W	X	Y	Ż	Ź

- tekst tajny $\mathbf{P} = \text{kryptografia} \mapsto \mathbf{C} = \text{HOWŃSMDOCCFC}$,
tekst jawny $\mathbf{C} = \text{MZOMLC} \mapsto \mathbf{P} = \text{obrona}$,
- kryptoanaliza wyczerpująca: od $|\Sigma_C|$ (dla $|\alpha| = 1$) do $|\Sigma_C|!$ (dla $|\alpha| = |\Sigma_C|$) przypadków.

Losowa permutacja alfabetu Σ_C :

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
K	B	Z	D	Ś	M	E	G	Ł	N	Ę	H	'_'	R	X	C	A
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
F	Ó	P	L	T	W	S	Ń	Ż	Ź	Y	Ą	Ć	I	U	O	J

- tekst tajny $\mathbf{P} =$ kryptografia $\mapsto \mathbf{C} = \text{RWĆTŻPNWKŁHK}$,
tekst jawny $\mathbf{C} = \text{KŻKR} \mapsto \mathbf{P} =$ atak,
- kryptoanaliza wyczerpująca: $|\Sigma_C|!$ przypadków, dla $|\Sigma_C| = 34$ otrzymujemy $34! \approx 2,952 \cdot 10^{38}$ (jeden przypadek na sekundę $\mapsto 9,362 \cdot 10^{30}$ lat).

Szyfr Vigenere'a - charakterystyka:

- szyfr podstawieniowy polialfabetyczny,
- macierz podstawień zgodna z tablicą Trithemiusa tj. przesunięcie alfabetu tekstu jawnego o $1 \leq k \leq |\Sigma_C|$ znaków w k -tym wierszu macierzy,
- użycie słowa kluczowego $\alpha \in \Sigma_C^*$.

Użycie słowa kluczowego $\alpha = \text{KOT}$:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
K	L	ł	M	N	ń	O	ó	P	R	S	ś	T	U	W	X	Y
O	ó	P	R	S	ś	T	U	W	X	Y	Z	ż	ź	' '	A	Ą
T	U	W	X	Y	Z	ż	ź	' '	A	Ą	B	C	Ć	D	E	Ę
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
Z	ż	ź	' '	A	Ą	B	C	Ć	D	E	Ę	F	G	H	I	J
B	C	Ć	D	E	Ę	F	G	H	I	J	K	L	ł	M	N	ń
F	G	H	I	J	K	L	ł	M	N	ń	O	ó	P	R	S	ś

- tekst tajny $\mathbf{P} = \text{kryptografia} \mapsto \mathbf{C} = \text{UĘÓAHHRETPZT}$,
tekst jawny $\mathbf{C} = \text{DŚŻĄŁZZZZ} \mapsto \mathbf{P} = \text{uderzenie}$,
- kryptoanaliza wyczerpująca: $|\Sigma_{\mathbf{C}}|^{|\alpha|}$ przypadków, dla $|\alpha| = |\Sigma_{\mathbf{C}}| = 34$ otrzymujemy $34^{34} \approx 1,176 \cdot 10^{52}$ (liczba atomów we Wszechświecie szacowana jest na 10^{81}).

Szyfr Playfaira - charakterystyka:

- szyfr podstawieniowy monodiagramowy,
- macierz podstawień wymiaru 5×5 ,
- użycie słowa kluczowego $\alpha \in \Sigma_C^*$ takiego, że

$$\forall i, j \in \{1, 2, \dots, |\alpha|\} : i \neq j \Rightarrow \alpha[i] \neq \alpha[j],$$

- reguły szyfrowania diagramów: liniowa (prawy sąsiad albo dolny sąsiad) i krzyżowa (przecięcie wiersza i kolumny),
- reguły odszyfrowania diagramów: liniowa (lewy sąsiad albo górny sąsiad) i krzyżowa (przecięcie wiersza i kolumny),

Użycie słowa kluczowego $\alpha = \text{STOLARZ}$:

S / Ś	T	O / Ó	L / Ł	A / Ą
R	Z / Ż / Ź	B	C/ Ć	D
E/ Ę	F	G	H	I
J	K	M	N/ Ń	P
U	W	X	Y	'_'

- tekst tajny $\mathbf{P} = \text{kryptografia} = \text{kr yp to gr af ia} \mapsto \mathbf{C} = \text{JZ_N OL EB TI PD} = \text{JZ_NOLEBTIPD}$,
tekst jawny $\mathbf{C} = \text{YREFDB} = \text{YR EF DB PT} \mapsto \mathbf{P} = \text{uc ie cz ka} = \text{ucieczka}$,
- kryptoanaliza wyczerpująca (zakładając przedstawione zlepienia liter): od 5^2 (dla $|\alpha| = 1$) do $(5^2)! \approx 1,551 \cdot 10^{25}$ (dla $|\alpha| = 5^2$) przypadków.

Kryptoanaliza szyfru Cezara:

- atak przez analizę częstości występowania znaków (tzw. analiza arabska),
- częstość występowania znaków w języku polskim:

a	0,078	g	0,012	ń	0,001	w	0,037
ą	0,010	h	0,011	o	0,061	x	0,000
b	0,012	i	0,077	ó	0,007	y	0,031
c	0,036	j	0,018	p	0,025	z	0,055
ć	0,004	k	0,025	r	0,037	ż	0,008
d	0,029	l	0,017	s	0,037	ź	0,001
e	0,064	ł	0,024	ś	0,006	' '	0,140
ę	0,013	m	0,023	t	0,029		
f	0,001	n	0,043	u	0,018		

Tekst jawny:

C = C_ORGŻGAIYXYEGŻDGALŻOXŻAJNOJŃŻALAŻYPMGR_JŻ_CJŻI_WŻOM-
YJBLŻIJE_ĘŻOJEŻOXCAĞŻN_WŻPGR_JŻAOGŻI_WŻNOMLI_ĆŻPY_ŃŻŁ_WAŁE-
GŃĘŻORUŻRŻILĆJAŻGYPG_B_JŻR_PYWŻ_ŻGŁ_NÓAWŻBGŻOWNAŁE_WŻŁGŻO-
GB_JŻŁLEEGŻŃR_WOLŻIGŻALNEJAŻBMGE_NYŻIYWNOGIKGRXŻ_ŻRŻGNOM-
JAŻŃR_JI_NYŻBMLD_JŻOXŻIGŻTMHPŻYLDĄGRXŻEGRGTMHPYAŻ_ŻGIKMŁE-
_LNYŻYŻAJTGŻR_JMEXDŻCÓPJDŻALAŻDE_JŻPY_JIĄGŻPGŻYPMGR_LŻŁGR-
MHI_ĆLNŻIÓPJDŻTPXŻGPŻŁĆLIYUIJAŻDŁOĄ_ŻŁGPŻORG AUŻGŁ_JAŁWŻGS_-
LMGRLEXŻDLMORUŻŁGPE_GNĆJDŻŁGR_JAŁWŻ_ŻYLMŁYŻDGTĆJDŻŁ_JNYG-
ŻPGŻORXIKŻŃR_UOXFŻŁMGTÓŻ_ŃĘŻYLŻRMHIGEJŻZXI_JŻŁGPY_WAŁGRŁĘ-
ŻBGTÓŻOLAŻELNŻŁGRMHI_NYŻIÓPJDŻELŻGAIYXYEXŻĆGEGŻOXDIYLNJD-
ŻŁMYJEGŃŻDGAUŻPÓNYWŻÓOWNAŁE_GEUŻPGŻOXIKŻŁLTHMAŁHRŻCJŃEX-
IKŻPGŻOXIKŻĆUAŻY_JCGEXIKŻNYJMGĄGŻELPŻBĆWAŁ_OEXDŻE_JDEJDŻMG-
YI_UTE_GEXIKŻPGŻOXIKŻŁHCŻDLCGRLEXIKŻYBGZJDŻMGYDL_OJDŻRXYĆ-
LILEXIKŻŁNYJE_IUŻŁGNMJBMYLEXIKŻZXOJDŻTPY_JŻBÓMNYOXEGRXŻŃR-
_JMYGŁŻTMXAŁŻALAŻŃE_JTŻŻB_LĆLŻTPY_JŻŁLE_JFNAŁ_DŻMÓD_JFIJDŻP-
Y_WI_JC_ELŻŁLĆLŻLŻRNYXNOAĞŻŁMYJŁLNLEJŻALAŁBXŻRNOWTUŻD_JPY-
UŻY_JCGEUŻELŻE_JAŻYŻMYLPAŁŻI_IKJŻTMÓNYJŻN_JPYU

- częstość występowania znaków w tekście jawnym:

A	0,019	G	0,075	Ń	0,013	W	0,019
Ą	0,027	H	0,008	O	0,034	X	0,034
B	0,014	I	0,042	Ó	0,012	Y	0,052
C	0,011	J	0,062	P	0,032	Z	0,003
Ć	0,013	K	0,014	R	0,033	Ż	0,000
D	0,030	L	0,054	S	0,001	Ź	0,154
E	0,046	Ł	0,025	Ś	0,000	' _ '	0,070
Ę	0,004	M	0,034	T	0,016		
F	0,003	N	0,031	U	0,015		

- zbieżność częstości znaków ' ' (0,140) oraz Ź (0,154), $\hat{Z} \mapsto ' '$,

Tekst jawny (podstawienie I):

C = C_ORG GAIYXYEG DGAL OX AJNOJŃ ALĄ YPMGR_J _CJ I_W OMYJBL
IJE_Ę OJE OXCĄG N_W PGR_J AOG I_W NOMLI_Ć PY_Ń Ł_WAEGŃĘ ORU RIL-
ĆJA GYPGB_J R_PYW _ GŁ_NÓAW BG OWNĄE_W ŁG OGB_J ŁLEEG ŃR_WOL
IG ALNEJA BMGE_NY IYWNOGIKGRX _ R GNOMJA ŃR_JI_NY BMLD_J OX
IG TMHP YLDĄGRX EGRGTMHPYĄ_ GIKMLE_LNY Y AJTG R_JMEXD CÓ-
PJD ALĄ DE_J PY_JIĄG PG YPMGR_L ŁGRMHI_ĆLŃ IÓPJD TPX GP ŁĆLIY-
UIJA DLOĄ_ ŁGP ORGAU GŁ_JĄW GS_LMGRLEX DLMORU ŁGPE_GNĆJD
ŁGR_JĄW _ YLMLY DGTĆJD Ł_JNYG PG ORXIK ŃR_UOXF ŁMGTÓ _ŃĘ
YL RMHIGEJ ZXI_J ŁGPY_WĄGRLE BGTÓ OLA_ ELN ŁGRMHI_NY IÓPJD EL
GAIYXYEX ĆGEG OXDIYLNJD ŁMYJEGŃ DGAU PÓNYW ÓOWNĄE_GEU PG
OXIK ŁLTHMAHR CJŃEXIK PG OXIK ĆUA_ Y_JCGEXIK NYJMGĄG ELP BĆWA_-
OEXD E_JDEJD MGYI_UTE_GEXIK PG OXIK ŁHC DLCGRLEXIK YBGZJD MG-
YDL_OJD RXYĆLILEXIK ŁNYJE_IU ŁGNMJBMYLEXIK ZXOJD TPY_J BÓM-
NYOXEGRX ŃR_JMYGŁ TMXAŁ ALĄ ŃE_JT B_LĆL TPY_J ŁLE_JFNA_ D MÓD-
_JFIJD PY_WI_JC_EL ŁLĆL L RNYXNOĄG ŁMYJŁLNLEJ ALĄBX RNOWTU
D_JPYU Y_JCGEU EL E_JA Y MYLPĄŁ I_IKJ TMÓNYJ N_JPYU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	Ż

- szukamy słów odpowiadających do i od oraz innego słowa dwulite-
rowego zawierającego literę odpowiadającą o,

$C = C_ORG$ GAIYXYEG DGAL OX AJNOJŃ ALĄ YPMGR_J _CJ I_W OMYJBL
 IJE_Ę OJE OXCAĞ N_W PGR_J AOG I_W NOMLI_Ć PY_Ń Ł_WAEGŃĘ ORU R IL-
 ĆJA GYPGB_J R_PYW _ GŁ_NÓAW BG OWNĄE_W **ŁG** OGB_J ŁLEEG ŃR_WOL
 IG ALNEJA BMGE_NY IYWNOGIKGRX _ R GNOMJA ŃR_JI_NY BMLD_J OX
 IG TMHP YLDAĞRX EGRGTMHPYĄ_ GIKMLE_LNY Y AJTG R_JMEXD CÔ-
 PJD ALĄ DE_J PY_JIĄG PG YPMGR_L ŁGRMHI_ĆLŃ IÓPJD TPX **GP** ŁĆLIY-
 UIJA DLOĄ_ ŁGP ORGAU GŁ_JAW GS_LMGRLEX DLMORU ŁGPE_GNĆJD
 ŁGR_JAW _ YLMLY DGTĆJD Ł_JNYG PG ORXIK ŃR_UOXF ŁMGTÓ _ŃĘ
 YL RMHIGEJ ZXI_J ŁGPY_WAĞRLĘ BGTÓ OLA_ ELN ŁGRMHI_NY IÓPJD EL
 GAIYXYEX ĆGEG OXDIYLNJD ŁMYJEGŃ DGAU PÓNYW ÓOWNĄE_GEU PG
 OXIK ŁLTHMAHR CJŃEXIK PG OXIK ĆUA_ Y_JCGEXIK NYJMGĄG ELP BĆWA_-
 OEXD E_JDEJD MGYI_UTE_GEXIK **PG** OXIK ŁHC DLCGRLEXIK YBGZJD MG-
 YDL_OJD RXYĆLILEXIK ŁNYJE_IU ŁGNMJBMYLEXIK ZXOJD TPY_J BÔM-
 NYOXEGRX ŃR_JMYGŁ TMXAŁ ALĄ ŃE_JT B_LĆL TPY_J ŁLE_JFNA_D MÔD-
 _JFIJD PY_WI_JC_EL ŁLĆL L RNYXNOĄG ŁMYJŁLNLEJ ALĄBX RNOWTU
 D_JPYU Y_JCGEU EL E_JA Y MYLPĄL I IKJ TMÓNYJ N_JPYU

- wnioskujemy: ŁG , GP i $\text{PG} \Rightarrow P$ odpowiada d oraz G odpowiada o ,
 $P \mapsto d$, $G \mapsto o$,

Tekst jawny (podstawienie II):

C = C_ORo oAIYXYEo DoAL OX AJNOJŃ ALA YdMoR_J _CJ I_W OMYJBL
IJE_Ę OJE OXCAo N_W doR_J AŃo I_W NOMLI_Ć dY_Ń Ł_WAEOŃĘ ORU R
ILĆJA oYdoB_J R_dYW _ oŁ_NÓAW Bo OWNAE_W Ło OoB_J ŁLEEo ŃR_WOL
Io ALNEJA BMoE_NY IYWNOoIKoRX _ R oNOMJA ŃR_JI_NY BMLD_J OX Io
TMHd YLDAoRX EoRoTMHdYA_ oIKMLE_LNY Y AJTo R_JMEXD CŃdJD ALA
DE_J dY_JIAo do YdMoR_L ŁoRMHI_ĆLŃ IŃdJD TdX od ŁĆLIYUIJA DLOA_ Łod
ORoAU oŁ_JAW oS_LMoRLEX DLMORU ŁodE_oŃĆJD ŁoR_JAW _ YLMLY Do-
TĆJD Ł_JNYo do ORXIK ŃR_UOXF ŁMoTÓ _ŃĘ YL RMHIoEJ ZXI_J ŁodY_WA_o-
RLĘ BoTÓ OLA_ ELN ŁoRMHI_NY IŃdJD EL oAIYXYEX ĆoEo OXDIYLNJD
ŁMYJEoŃ DoAU dŃNYW ŐOWNAE_oEU do OXIK ŁLTHMAHR CJŃEXIK do
OXIK ĆUA_ Y_JCoEXIK NYJMoA_o ELd BĆWA_OEXD E_JDEJD MoYI_UTE_oEXIK
do OXIK ŁHC DLCoRLEXIK YBoZJD MoYDL_OJD RXYĆLILEXIK ŁNYJE_IU
ŁoNMJBMYLEXIK ZXOJD TdY_J BŐMNYOXEoRX ŃR_JMYoŁ TMXAŁ ALA
ŃE_JT B_LĆL TdY_J ŁLE_JFNA_D MŐD_JFIJD dY_WI_JC_EL ŁLĆL L RNY-
XNOA_o ŁMYJŁLNLEJ ALAXBX RNOWTU D_JdYU Y_JCoEU EL E_JA Y MYLdAŁ
I_IKJ TMŐNYJ N_JdYU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
?	?	?	?	?	P	?	?	?	?	?	?	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	?	?	?	?	?	?	?	?	?	?	?	?	Ż

- szukamy odpowiedników słów z i w oraz słów umożliwiających stwierdzenie, które z pojedynczych słów tekstu jawnego jest spółgłoską,

C = C_ORo oAIYXYEo DoAL OX AJNOJŃ ALA YdMoR_J _CJ I_W OMYJBL
 IJE_Ę OJE OXCAo N_W doR_J AŃo I_W NOMLI_Ć dY_Ń Ł_WAĘoŃĘ ORU R
 ILĆJA oYdoB_J R_dYW _ oŁ_NŌAW Bo OWNĄE_W Ło OoB_J ŁLEEo ŃR_WOL
 Io ALNEJA BMoE_NY IYWNOoIKoRX _ R oNOMJA ŃR_JI_NY BMLD_J OX Io
 TMHd YLDAoRX EoRoTMHdYA_ oIKMLE_LNY Y AJTo R_JMEXD CŌdJD ALA
 DE_J dY_JIAo do YdMoR_L ŁoRMHI_ĆLŃ IŌdJD TdX od ŁĆLIYUIJA DLOA_ Łod
 ORoAU oŁ_JA_W oS_LMoRLEX DLMORU ŁodE_oŃĆJD ŁoR_JA_W _ YLMLY Do-
 TĆJD Ł_JNYo do ORXIK ŃR_UOXF ŁMoTŌ _ŃĘ YL RMHIoEJ ZXI_J ŁodY_WA_o-
 RLĘ BoTŌ OLA ELN ŁoRMHI_NY IŌdJD EL oAIYXYEX ĆoEo OXDIYLNJD
 ŁMYJEoŃ DoAU dŌNYW ŌOWNĄE_oEU do OXIK ŁLTHMAHR CJŃEXIK do
 OXIK ĆUA_Y_JCoEXIK NYJMoA_o ELd BĆWA_OEXD E_JDEJD MoYI_UTE_oEXIK
 do OXIK ŁHC DLCoRLEXIK YBoZJD MoYDL_OJD RXYĆLILEXIK ŁNYJE_IU
 ŁoNMJBMYLEXIK ZXOJD TdY_J BŌMNYOXEoRX ŃR_JMYoŁ TMXAŁ ALA
 ŃE_JT B_LĆL TdY_J ŁLE_JFNA_D MŌD_JFIJD dY_WI_JC_EL ŁLĆL L RNY-
 XNOA_o ŁMYJŁLNLEJ ALABX RNOWTU D_JdYU Y_JCoEU EL E_JA Y MYLdAŁ
 I_IKJ TMŌNYJ N_JdYU

- wnioskujemy: C_ORo , doR_J i _ \Rightarrow R jest spółgłoską, zbieżność częstości znaków w (0,037) oraz R (0,033), $R \mapsto w$,

Tekst jawny (podstawienie III):

C = C_Owo oAIYXYEo DoAL OX AJNOJŃ ALA YdMow_J _CJ I_W OMYJBL
IJE_Ę OJE OXCAo N_W dow_J AŃo I_W NOMLI_Ć dY_Ń Ł_WAEOŃĘ OwU w
ILĆJA oYdoB_J w_dYW _ oŁ_NÓAW Bo OWNAE_W Ło OoB_J ŁLEEo Ńw_WOL
Io ALNEJA BMoE_NY IYWNOoIKowX _ w oNOMJA Ńw_JI_NY BMLD_J OX Io
TMHd YLDAowX EowoTMHdYA_ oIKMLE_LNY Y AJTo w_JMEXD CŃdJD ALA
DE_J dY_JIAo do YdMow_L ŁowMHI_ĆLŃ IŃdJD TdX od ŁĆLIYUIJA DLOA_ Łod
OwoAU oŁ_JAW oS_LMowLEX DLMOWU ŁodE_oNĆJD Łow_JAW _ YLMLY Do-
TĆJD Ł_JNYo do OwXIK Ńw_UOXF ŁMoTÓ _ŃĘ YL wMHioEJ ZXI_J ŁodY_WAo-
wLE_ BoTÓ OLA_ ELN ŁowMHI_NY IŃdJD EL oAIYXYEX ĆoEo OXDIYLNJD
ŁMYJEoŃ DoAU dŃNYW ŐOWNAE_oEU do OXIK ŁLTHMAHw CJŃEXIK do
OXIK ĆUA_ Y_JCoEXIK NYJMoAo ELd BĆWA_OEXD E_JDEJD MoYI_UTE_oEXIK
do OXIK ŁHC DLCowLEXIK YBoZJD MoYDL_OJD wXYĆLILEXIK ŁNYJE_IU
ŁoNMJBMYLEXIK ZXOJD TdY_J BŐMNYOXEowX Ńw_JMYoŁ TMXAŁ ALA
ŃE_JT B_LĆL TdY_J ŁLE_JFNA_D MŐD_JFIJD dY_WI_JC_EL ŁLĆL L wNY-
XNOAo ŁMYJŁLNLEJ ALAXBX wNOWTU D_JdYU Y_JCoEU EL E_JA Y MYLdAŁ
I_IKJ TMŐNYJ N_JdYU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
?	?	?	?	?	P	?	?	?	?	?	?	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	?	?	?	?	?	?	R	?	?	?	?	?	Ż

- szukamy słów odpowiadających co, go , no, po albo to oraz innych słów zawierających te dwuliterowe wyrazy,

$C = C_Owo \ oAIYXYEo \ DoAL \ OX \ AJNOJ\acute{N} \ ALA\grave{A} \ YdMow_J \ _CJ \ I_W \ OMYJBL$
 $IJE_E \ OJE \ OXCA\grave{o} \ N_W \ dow_J \ A\grave{o}o \ I_W \ NOMLI_C \ dY_N \ _WAEo\acute{N}E \ OwU \ w$
 $IL\acute{C}JA \ oYdoB_J \ w_dYW \ _o__L_N\acute{O}AW \ Bo \ OWN\grave{A}E_W \ _Lo \ OoB_J \ _LEEO \ \acute{N}w_WOL$
 $Io \ ALNEJA \ BMoE_NY \ IYWNOoIKowX \ _w \ oNOMJA \ \acute{N}w_JI_NY \ BMLD_J \ OX \ Io$
 $TMHd \ YLDA\grave{o}wX \ EowoTMHdYA\grave{A} \ _oIKMLE_LNY \ Y \ AJTo \ w_JMEXD \ C\acute{O}dJD \ ALA\grave{A}$
 $DE_J \ dY_JIA\grave{o} \ do \ YdMow_L \ _lowMHI_C\acute{L}\acute{N} \ I\acute{O}dJD \ TdX \ od \ _C\acute{L}IYUIJA \ DLOA\grave{A} \ _lod$
 $OwoAU \ o__JAW \ oS_LMowLEX \ DLMOWU \ _odE_oN\acute{C}JD \ _low_JAW \ _YLMLY \ Do-$
 $T\acute{C}JD \ _JNYo \ do \ OwXIK \ \acute{N}w_UOXF \ _LMoT\acute{O} \ _N\acute{E} \ YL \ wMHIoEJ \ ZXI_J \ _odY_WA\grave{o}-$
 $wL\acute{E} \ BoT\acute{O} \ OLA\grave{A} \ ELN \ _lowMHI_NY \ I\acute{O}dJD \ EL \ oAIYXYEX \ \acute{C}oEo \ OXDIYLNJD$
 $_LMYJEo\acute{N} \ DoAU \ d\acute{O}NYW \ \acute{O}OWN\grave{A}E_oEU \ do \ OXIK \ _LTHMA\grave{H}w \ CJ\acute{N}EXIK \ do$
 $OXIK \ \acute{C}UA\grave{A} \ Y_JCoEXIK \ NYJM\grave{o}A\grave{o} \ ELd \ B\acute{C}WA\grave{A} \ OEXD \ E_JDEJD \ MoYI_UTE_oEXIK$
 $do \ OXIK \ _LHC \ DLCowLEXIK \ YBoZJD \ MoYDL_OJD \ wXY\acute{C}LILEXIK \ _NYJE_IU$
 $_oNMJBMYLEXIK \ ZXOJD \ TdY_J \ B\acute{O}MN\grave{Y}OXEowX \ \acute{N}w_JMYo__ \ TMXA\grave{L} \ ALA\grave{A}$
 $\acute{N}E_JT \ B_L\acute{C}L \ TdY_J \ _LE_JFNA\grave{A} _D \ M\acute{O}D_JFIJD \ dY_WI_JC_EL \ _L\acute{C}L \ L \ wNY-$
 $XNOA\grave{o} \ _LMYJ__LNLEJ \ ALA\grave{B}X \ wNOWTU \ D_JdYU \ Y_JCoEU \ EL \ E_JA \ Y \ MYLdA\grave{L}$
 $I_IKJ \ TM\acute{O}NYJ \ N_JdYU$

- wnioskujemy: $_lo \ i \ _low_JAW \Rightarrow _l$ odpowiada n , p albo t , zbieżność częstości znaków p $(0,025)$ oraz $_l$ $(0,025)$, $_l \longmapsto p$,

Tekst jawny (podstawienie IV):

C = C_Owo oAIYXYEo DoAL OX AJNOJŃ ALA YdMow_J _CJ I_W OMYJBL
IJE_Ę OJE OXCAo N_W dow_J AŃOo I_W NOMLI_Ć dY_Ń p_WAEOŃĘ OwU w
ILĆJA oYdoB_J w_dYW _ op_NÓAW Bo OOWNAŁE_W po OoB_J pLEEo Ńw_WOL
Io ALNEJA BMoE_NY IYWNOoIKowX _ w oNOMJA Ńw_JI_NY BMLD_J OX Io
TMHd YLDAowX EowoTMHdYA_ oIKMLE_LNY Y AJTo w_JMEXD CŃdJD ALA
DE_J dY_JIAo do YdMow_L powMHI_ĆLŃ IŃdJD TdX od pĆLIYUIJA DLOA_ pod
OwoAU op_JAW oS_LMowLEX DLMOWU podE_oNĆJD pow_JAW _ YLMLY Do-
TĆJD p_JNYo do OwXIK Ńw_UOXF pMoTŃ _ŃĘ YL wMHioEJ ZXI_J podY_WAow-
LĘ BoTŃ OLA ELN powMHI_NY IŃdJD EL oAIYXYEX ĆoEo OXDIYLNJD pMY-
JEOŃ DoAU dŃONYW ŃOOWNAŁE_oEU do OXIK pLTHMAHw CJŃEXIK do OXIK
ĆUA Y_JCoEXIK NYJMoAo ELd BĆWA_OEXD E_JDEJD MoYI_UTE_oEXIK do
OXIK pHc DLCowLEXIK YBoZJD MoYDL_OJD wXYĆLILEXIK pNYJE_IU poNM-
JBMYLEXIK ZXOJD TdY_J BŃMNYOXEowX Ńw_JMYop TMXAŁ ALA ŃE_JT
B_LĆL TdY_J pLE_JFNA_D MŃD_JFIJD dY_WI_JC_EL pLĆL L wNYXNOAo pMY-
JpLNLEJ ALABX wNOWTU D_JdYU Y_JCoEU EL E_JA Y MYLdAŁ I_IKJ TMŃ-
NYJ N_JdYU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
?	?	?	?	?	P	?	?	?	?	?	?	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	Ł	?	?	?	?	?	R	?	?	?	?	?	Ż

- szukamy odpowiedników słowa z i przyrostków odpowiadających owie oraz słów umożliwiających stwierdzenie, które z pojedynczych słów tekstu jawnego jest spółgłoską,

$C = C_Owo \ oAIYXYEo \ DoAL \ OX \ AJNOJ\acute{N} \ AL\acute{A} \ YdMow_J \ _CJ \ I_W \ OMYJBL$
 $IJE_E \ OJE \ OXCAo \ N_W \ dow_J \ A\acute{O}o \ I_W \ NOMLI_C \ dY_N \ p_WA\acute{E}o\acute{N}\acute{E} \ OwU \ w$
 $IL\acute{C}JA \ oYdoB_J \ w_dYW \ _op_N\acute{O}AW \ Bo \ OWN\acute{A}\acute{E}_W \ po \ OoB_J \ pLEEo \acute{N}w_WOL$
 $Io \ ALNEJA \ BMoE_NY \ IYWNOoIKowX \ _w \ oNOMJA \acute{N}w_JI_NY \ BMLD_J \ OX \ Io$
 $TMHd \ YLDA\acute{o}wX \ EowoTMHdYA\acute{A} \ _oIKMLE_LNY \ Y \ AJTo \ w_JMEXD \ C\acute{O}dJD \ AL\acute{A}$
 $DE_J \ dY_JIA\acute{o} \ do \ YdMow_L \ powMHI_C\acute{L}\acute{N} \ I\acute{O}dJD \ TdX \ od \ p\acute{C}LIYUIJA \ DLO\acute{A} \ _pod$
 $OwoAU \ op_JA\acute{W} \ oS_LMowLEX \ DLMOwU \ podE_oN\acute{C}JD \ pow_JA\acute{W} \ _YLMLY \ Do-$
 $T\acute{C}JD \ p_JNYo \ do \ OwXIK \acute{N}w_UOXF \ pMoT\acute{O} \ _N\acute{E} \ YL \ wMHIoEJ \ ZXI_J \ podY_WA\acute{o}w-$
 $LE\acute{A} \ BoT\acute{O} \ OL\acute{A} \ ELN \ powMHI_NY \ I\acute{O}dJD \ EL \ oAIYXYEX \ C\acute{o}Eo \ OXDIYLNJD \ pMY-$
 $JEo\acute{N} \ DoAU \ d\acute{O}NYW \acute{O}OWN\acute{A}\acute{E}_oEU \ do \ OXIK \ pLTHMA\acute{H}w \ CJ\acute{N}EXIK \ do \ OXIK$
 $\acute{C}UA\acute{A} \ Y_JCoEXIK \ NYJMo\acute{A}o \ ELd \ B\acute{C}WA\acute{A} \ OEXD \ E_JDEJD \ MoYI_UTE_oEXIK \ do$
 $OXIK \ pHC \ DLCowLEXIK \ YBoZJD \ MoYDL_OJD \ wXY\acute{C}LILEXIK \ pNYJE_IU \ poNM-$
 $JBMYLEXIK \ ZXOJD \ TdY_J \ B\acute{O}MNYOXEowX \acute{N}w_JMYop \ TMXA\acute{L} \ AL\acute{A} \acute{N}E_JT$
 $B_L\acute{C}L \ TdY_J \ pLE_JFNA\acute{A} \ D \ M\acute{O}D_JFIJD \ dY_WI_JC_EL \ pL\acute{C}L \ L \ wNYXNO\acute{A}o \ pMY-$
 $JpLNLEJ \ AL\acute{A}BX \ wNOWTU \ D_JdYU \ Y_JCoEU \ EL \ E_JA \ Y \ MYLd\acute{A}L \ I_IKJ \ TM\acute{O}-$
 $NYJ \ N_JdYU$

- wnioskujemy: Y i $oYdoB_J \Rightarrow Y$ odpowiada z , $YdMow_J$, dow_J i zbieżność częstości znaków e (0,064) oraz J (0,062), $Y \mapsto z$, $J \mapsto e$,

Tekst jawny (podstawienie V):

C = C_Owo oAIzXzEo DoAL OX AeNOeŃ ALĄ zdMow_e _Ce I_W OMzeBL
IeE_Ę OeE OXCAo N_W dow_e A_Oo I_W NOMLI_Ć dz_Ń p_WAĘoŃĘ OwU w
ILĆeA ozdoB_e w_dzW _ op_NÓAW Bo OOWNĄE_W po OoB_e pLEEO Ńw_WOL
Io ALNEeA BMoE_Nz IzWNOoIKowX _ w oNOMeA Ńw_eI_Nz BMLD_e OX Io
TMHd zLDAowX EowoTMHdzA_ oIKMLE_LNz z AeTo w_eMEXD CÓdeD ALĄ
DE_e dz_eIAo do zdMow_L powMHI_ĆLŃ IÓdeD TdX od pĆLIzUIeA DLOA_ pod
OwoAU op_eAW oS_LMowLEX DLMOWU podE_oNĆeD pow_eAW _ zLMLz Do-
TĆeD p_eNzo do OwXIK Ńw_UOXF pMoTÓ _ŃĘ zL wMHIOeE ZXI_e podz_WAowLE
BoTÓ OLA_ ELN powMHI_Nz IÓdeD EL oAIzXzEX ĆoEo OXDIZLNeD pMzeEoŃ
DoAU dÓNzW ÓOWNĄE_oEU do OXIK pLTHMAHw CeŃEXIK do OXIK ĆUA_
z_eCoEXIK NzeMoAo ELd BĆWA_OEXD E_eDEeD MozI_UTE_oEXIK do OXIK
pHC DLCowLEXIK zBoZeD MozDL_OeD wXzĆLILEXIK pNzeE_IU poNMeBM-
zLEXIK ZXOeD Tdz_e BÓMNzOXEowX Ńw_eMzop TMXAŁ ALĄ ŃE_eT B_LĆL
Tdz_e pLE_eFNA_D MÓD_eFIeD dz_WI_eC_EL pLĆL L wNzXNOAo pMzepLNLEe
ALĄBX wNOWTU D_edzU z_eCoEU EL E_eA z MzLdAŁ I_IKe TMÓNze N_edzU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
?	?	?	?	?	P	J	?	?	?	?	?	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	Ł	?	?	?	?	?	R	?	?	Y	?	?	Ż

- szukamy odpowiedników słowa i i a oraz innych słów zawierających te jednoliterowe wyrazy,

$C = C_Owo \ oAizXzEo \ DoAL \ OX \ AeNOe\acute{N} \ ALA\grave{A} \ zdMow_e \ _Ce \ I_W \ OMzeBL$
 $IeE_E \ OeE \ OXCA\grave{o} \ N_W \ \text{dow_e} \ A\grave{O}o \ I_W \ NOMLI_C \ dz_N \ p_WA\grave{E}o\acute{N}\grave{E} \ OwU \ w$
 $IL\acute{C}eA \ ozdoB_e \ w_dzW \ _op_N\acute{O}AW \ Bo \ OWN\grave{A}\grave{E}_W \ po \ OoB_e \ pLEEo \acute{N}w_WOL$
 $Io \ ALNEeA \ BMoE_Nz \ IzWNOoIKowX \ _w \ oNOMeA \acute{N}w_eI_Nz \ BMLD_e \ OX \ Io$
 $TMHd \ zLDA\grave{o}wX \ EowoTMHdz\grave{A}_ \ oIKMLE_LNz \ z \ AeTo \ w_eMEXD \ C\acute{O}deD \ ALA\grave{A}$
 $DE_e \ dz_eI\grave{A}\grave{o} \ do \ zdMow_L \ powMHI_C\acute{L}\acute{N} \ I\acute{O}deD \ TdX \ od \ p\acute{C}LIzUIeA \ DLO\grave{A}_ \ pod$
 $OwoAU \ op_e\grave{A}_W \ oS_LMowLEX \ DLMOWU \ podE_oN\acute{C}eD \ pow_e\grave{A}_W \ _zLMLz \ Do-$
 $T\acute{C}eD \ p_eNzo \ do \ OwXIK \acute{N}w_UOXF \ pMoT\acute{O} \ _N\grave{E} \ zL \ wMHioEe \ ZXI_e \ podz_WA\grave{o}wL\grave{E}$
 $BoT\acute{O} \ OLA\grave{A} \ ELN \ powMHI_Nz \ I\acute{O}deD \ EL \ oAizXzEX \ C\acute{o}Eo \ OXDizLNeD \ pMzeEo\acute{N}$
 $DoAU \ d\acute{O}NzW \acute{O}OWN\grave{A}\grave{E}_oEU \ do \ OXIK \ pLTHMA\grave{H}w \ Ce\acute{N}EXIK \ do \ OXIK \ C\acute{U}\grave{A}$
 $z_eCoEXIK \ NzeMo\grave{A}\grave{o} \ ELd \ B\acute{C}WA\grave{A} \ OEXD \ E_eDEeD \ MozI_UTE_oEXIK \ do \ OXIK$
 $pHC \ DLCowLEXIK \ zBoZeD \ MozDL_OeD \ wXz\acute{C}LILEXIK \ pNzeE_IU \ poNMeBM-$
 $zLEXIK \ ZXOeD \ Tdz_e \ B\acute{O}MNzOXEowX \acute{N}w_eMzop \ TMX\grave{A}_L \ ALA\grave{A} \acute{N}E_eT \ B_L\acute{C}L$
 $Tdz_e \ pLE_eFNA\grave{A} _D \ M\acute{O}D_eFIeD \ dz_WI_eC_EL \ pL\acute{C}L \ \text{L} \ wNzXNO\grave{A}\grave{o} \ pMzepLNLEe$
 $ALA\grave{B}X \ wNOWTU \ D_edzU \ z_eCoEU \ EL \ E_eA \ z \ MzLd\grave{A}_L \ I_IKe \ TM\acute{O}Nze \ N_edzU$

- wnioskujemy: $_ , L \ i \ dow_e \Rightarrow _ \text{ odpowiada } i \text{ oraz } L \text{ odpowiada } a, L$
 $\longmapsto a, _ \longmapsto i,$

Tekst jawny (podstawienie VI):

C = CiOwo oAIzXzEo DoAa OX AeNOeŃ AaĄ zdMowie iCe IiW OMzeBa IeEiĘ
OeE OXCAo NiW dowie AŃOo IiW NOMaIiĆ dziŃ piWAŃEoŃĘ OwU w IaĆeA ozdoBie
widzW i opiNÓAW Bo OOWNAŃEiW po OoBie paEEo ŃwiWOa Io AaNeeA BMoEiNz
IzWNOoIKowX i w oNOMeA ŃwieIiNz BMaDie OX Io TMHd zaDAŃowX EowoTMH-
dzAŃ oIKMaEiaNz z AeTo wieMEXD CŃdeD AaĄ DEie dzieIAŃ do zdMowia po-
wMHIIĆaŃ IŃdeD TdX od pĆaIzUIeA DaOAŃ pod OwoAU opieAŃW oSiaMowaEX
DaMOwU podEioNĆeD powieAŃW i zaMaz DoTĆeD pieNzo do OwXIK ŃwiUOXF
pMoTŃ iŃĘ za wMHIOeE ZXIe podziWAŃowaĘ BoTŃ OaĄ EaN powMHIIiNz IŃ-
deD Ea oAIzXzEX ĆoEo OXDIZAneD pMzeEoŃ DoAU dŃNzW ŃOWNAŃEioEU
do OXIK paTHMAŃHw CeŃEXIK do OXIK ĆUAŃ zieCoEXIK NzeMoAŃ Ead BĆWAŃ-
iOEXD EieDEeD MozIiUTEioEXIK do OXIK pHc DaCowaEXIK zBoZeD MozDa-
iOeD wXzĆaIaEXIK pNzeEiIU poNMeBMzaEXIK ZXOeD Tdzie BŃMNzOXEowX
ŃwieMzop TMXAŃ AaĄ ŃEieT BiaĆa Tdzie paEieFNAŃD MŃDieFieD dziWIIeCiEa
paĆa a wNzXNOAŃ pMzepaNaEe AaĄBX wNOWTU DiedzU zieCoEU Ea EieA z
MzadAŃ IiIKe TMŃNze NiedzU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	?	?	?	?	P	J	?	?	?	?	'_'	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	Ł	?	?	?	?	?	R	?	?	Y	?	?	Ż

- szukamy odpowiednika słowa co oraz inny słów zawierających ten dwuliterowy wyraz,

$C =$ CiOwo oAIZXzEo DoAa OX AeNOeŃ AaĄ zdMowie iCe IiW OMzeBa IeEiĘ
 OeE OXCAo NiW dowie AŃOo **IiW** NOMaIiĆ dziŃ piWAŃEoŃĘ OwU w IaĆeA ozdo-
 Bie **widzW** i opiNŃAW Bo OWNĄEiW po OoBie paEEo ŃwiWOa **Io** AaNeeA
 BMoEiNz IzWNOoIKowX i w oNOMeA ŃwieIiNz BMaDie OX Io TMHd zaDAowX
 EowoTMHdzAi oIKMaEiaNz z AeTo wieMEXD CŃdeD AaĄ DEie dzieIAo do zdMo-
 wia powMHİiĆaŃ IŃdeD TdX od pĆaIZUIeA DaOAi pod OwoAU opieAW oSiaMo-
 waEX DaMOwU podEioNĆeD powieAW i zaMaz DoTĆeD pieNzo do OwXIK ŃwiU-
 OXF pMoTŃ iŃĘ za wMHİoEe ZXİe podziWAowaĘ BoTŃ OaĄ EaN powMHİiNz
 IŃdeD Ea oAIZXzEX ĆoEo OXDİzaNeD pMzeEoŃ DoAU dŃNzW ŃOWNĄEioEU
 do OXIK paTHMAŃHw CeŃEXIK do OXIK ĆUA zieCoEXIK NzeMoAo Ead BĆWA-
 iOEXD EieDEeD MozİiUTEioEXIK do OXIK pHc DaCowaEXIK zBoZeD MozDa-
 iOeD wXzĆaİaEXIK pNzeEiIU poNMeBMzaEXIK ZXOeD Tdzie BŃMNzOXEowX
 ŃwieMzop TMXAa AaĄ ŃEieT BiaĆa Tdzie paEieFNAiD MŃDieFIeD dziWIieCiEa
 paĆa a wNzXNOAo pMzepaNaEe AaĄBX wNOWTU DiedzU zieCoEU Ea EieA z
 MzadAa İiİKe TMŃNze NiedzU

- wnioskujemy: Io , IiW i $widzW \Rightarrow I$ odpowiada c oraz w odpowiada e ,
 $I \longmapsto c$, $W \longmapsto e$,

Tekst jawny (podstawienie VII):

C = CiOwo oAczXzEo DoAa OX AeNOeŃ AaĄ zdMowie iCe cię OMzeBa ceEiĘ
OeE OXCAo Nię dowie ĄOo cię NOMaciĆ dziŃ pięĄEoŃĘ OwU w caĆeA ozdoBie
widzę i opiNŌAę Bo OęNAĘEię po OoBie paEEo ŃwieĄOa co AaNEEA BMoEiNz czę-
NOocKowX i w oNOMeA ŃwieciNz BMaDie OX co TMHd zaDAowX EowoTMH-
dzĄi ocKMaEiaNz z AeTo wieMEXD CŌdeD AaĄ DEie dziecĄo do zdMowia po-
wMHciĆaŃ cŌdeD TdX od pĆaczUceA DaOAi pod OwoAU opieĄę oSiaMowaEX
DaMOwU podEioNĆeD powieĄę i zaMaz DoTĆeD pieNzo do OwXcK ŃwiUOXF
pMoTŌ iŃĘ za wMHcoEe ZXcie podzieĄowaĘ BoTŌ OaĄ EaN powMHciNz cŌ-
deD Ea oAczXzEX ĆoEo OXDczaNeD pMzeEoŃ DoAU dŌNzę ŌOęNAĘEioEU do
OXcK paTHMAwHw CeŃEXcK do OXcK ĆUAz zieCoEXcK NzeMoĄo Ead BĆęAiO-
EXD EieDEeD MozciUTEioEXcK do OXcK pHc DaCowaEXcK zBoZeD MozDa-
iOeD wXzĆacaEXcK pNzeEicU poNMeBMzaEXcK ZXOeD Tdzie BŌMNzOXEowX
ŃwieMzop TMXAa AaĄ ŃEieT BiaĆa Tdzie paEieFNAiD MŌDieFceD dziećcieCiEa
paĆa a wNzXNOĄo pMzepaNaEe AaĄBX wNOęTU DiedzU zieCoEU Ea EieA z
MzadĄa cicKe TMŌNze NiedzU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	?	?	I	?	P	J	W	?	?	?	'_'	?	?	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
?	?	G	?	Ł	?	?	?	?	?	R	?	?	Y	?	?	Ż

- szukamy słów pozwalających jednoznacznie określić podstawienia,

$C =$ CiOwo oAczXzEo DoAa OX AeNOeń AaĄ zdMowie iCe cię OMzeBa ceEiĘ
 OeE OXCĄo Nię dowie ĄOo cię NOMaciĆ dziń pięĄEońĘ OwU w caĆeA **ozdoBie**
 widzę i opiNÓAę Bo OęNAĘEię po OoBie **paEEo** ŃwieĄo co AaNeeA BMoEiNz czę-
 NOocKowX i w oNOMeA ŃwieciNz BMaDie OX co TMHd zaDAówX EowoTMH-
 dzAi ockMaEiaNz z AeTo wieMEXD CÓdeD AaĄ DEie dziecĄo do zdMowia po-
 wMHciĆań cÓdeD TdX od pĆaczUceA DaOAi pod OwoAU opieĄę oSiaMowaEX
 DaMOwU podEioNĆeD **powieĄę** i zaMaz DoTĆeD pieNzo do OwXcK ŃwiUOXF
 pMoTÓ ińĘ za wMHcoEe ZXcie podzięĄowaĘ BoTÓ OaĄ EaN powMHciNz cÓ-
 deD Ea oAczXzEX ĆoEo OXDczaNeD pMzeEoń DoAU dÓNzę ÓOęNAĘEioEU do
 OXcK paTHMAųHw CeńEXcK do OXcK ĆUAų zieCoEXcK NzeMoĄo Ead BĆęAiO-
 EXD EieDEeD MozciUTEioEXcK do OXcK pHc DaCowaEXcK zBoZeD MozDa-
 iOeD wXzĆacaEXcK pNzeEicU poNMeBMzaEXcK ZXOeD Tdzie BÓMNzOXEowX
 ŃwieMzop TMXAų AaĄ ŃEieT BiaĆa Tdzie paEieFNAiD MÓDieFceD dzięcieCiEa
 paĆa a wNzXNOĄo pMzepaNaEe AaĄBX wNOęTU DiedzU zieCoEU Ea EieA z
 MzadAųa cicKe TMÓNze NiedzU

- \bullet $ozdoBie \Rightarrow B$ odpowiada b , $paEEo \Rightarrow E$ odpowiada n , $powieĄę \Rightarrow A$
 odpowiada k , $B \mapsto b$, $E \mapsto n$, $A \mapsto k$,

Tekst jawny (podstawienie VIII):

C = CiOwo oAczXzno DoAa OX AeNOeŃ Aak zdMowie iCe cię OMzeba cenieŃ Oen OXCko Nie dowie kOo cię NOMaciĆ dziŃ pięknoŃeŃ OwU w caĆeA ozdobie widzę i opiŃÓAę bo OęNknieŃ po Oobie panno ŃwieŃOa co AaNneA bMoniNz częNOocKowX i w oNOMeA ŃwieciNz bMaDie OX co TMHd zaDkowX nowoTMHdzki ocKManiaNz z AeTo wieMnXD CŌdeD Aak Dnie dziecko do zdMowia powMHciĆaŃ cŌdeD TdX od pĆaczUceA DaOki pod OwoAU opiekę oSiaMowanX DaMOwU podnioŃĆeD powiekę i zaMaz DoTĆeD pieNzo do OwXcK ŃwiUOXF pMoTŌ iŃeŃ za wMHcone ZXcie podziękowaę boTŌ Oak naN powMHciNz cŌdeD na oAczXznX Ćono OXD-czaNeD pMzenoŃ DoAU dŌNzę ŌOęNknionU do OXcK paTHMkHw CeŃnXcK do OXcK ĆUk zieConXcK NzeMoko nad bĆękiOnXD nieDneD MozciUTnionXcK do OXcK pHc DaCowanXcK zboZeD MozDaiOeD wXzĆacanXcK pNzenicU poN-MebMzanXcK ZXOeD Tdzie bŌMNzOXnowX ŃwieMzop TMXka Aak ŃnieT biaĆa Tdzie panieFNkiD MŌDieFceD dziećCina paĆa a wNzXNOko pMzepaNane AakbX wNOęTU DiedzU zieConU na nieA z Mzadka cicKe TMŌNze NiedzU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	?	B	I	?	P	J	W	?	?	?	'_'	?	A	?	?	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
E	?	G	?	Ł	?	?	?	?	?	R	?	?	Y	?	?	Ż

- szukamy słów pozwalających jednoznacznie określić podstawienia,

C = CiOwo oAczXzno DoAa OX AeNOeŃ Aak **zdMowie** iCe cię **OMzeba** ceniĘ
 Oen OXCko Nię dowie kOo cię **NOMaciĆ** dziŃ pięknoŃĘ OwU w caĆeA ozdobie
 widzę i opiŃÓAę bo OęNknię po **Oobie** panno ŃwieŃOa co AaNneA bMoniNz czę-
 NOocKowX i w oNOMeA ŃwieciNz bMaDie OX co TMHd zaDkowX nowoTMHdzki
 ocKManiaNz z AeTo wieMnXD CŃdeD Aak Dnie dziecko do zdMowia powMHciĆaŃ
 cŃdeD TdX od pĆaczUceA DaOki pod OwoAU opiekę oSiaMowanX DaMOwU pod-
 nioŃĆeD powiekę i **zaMaz** DoTĆeD pieŃzo do OwXcK ŃwiUOXF pMoTŃ iŃĘ za
 wMHcone ZXcie podziękowaĘ boTŃ Oak naN powMHciNz cŃdeD na oAczXznX
 Ćono OXDczaneD pMzenoŃ DoAU dŃNzę ŃOęNknionU do OXcK paTHMkHw
 CeŃnXcK do OXcK ĆUk zieConXcK NzeMoko nad bĆękiOnXD nieDneD Moz-
 ciUTnionXcK do OXcK pHc DaCowanXcK zboZeD MozDaiOeD wXzĆacanXcK
 pNzenicU poNMebMzanXcK ZXOeD Tdzie bŃMNzOXnowX ŃwieMzop TMXka
 Aak ŃnieT **biaĆa** Tdzie panieFNkiD MŃDieFceD dziecięCina paĆa a wNzXNOko
 pMzepaNane AakbX wNOęTU DiedzU zieConU na nieA z Mzadka cicKe TMŃNze
 NiedzU

- $\text{zdMowie} \text{ i } \text{zaMaz} \Rightarrow \text{M}$ odpowiada r , $\text{OMzeba} \text{ i } \text{Oobie} \Rightarrow \text{O}$ odpowiada t , $\text{NOMaciĆ} \text{ i } \text{biaĆa} \Rightarrow \text{Ć}$ odpowiada ł , oraz N odpowiada s ,
 $\text{M} \mapsto r$, $\text{O} \mapsto t$, $\text{Ć} \mapsto \text{ł}$, $\text{N} \mapsto s$,

Tekst jawny (podstawienie IX):

C = Citwo oAczXzno DoAa tX AesteŃ Aak zdrowie iCe cię trzeba ceniĘ ten tXCko się dowie kto cię stracił dziŃ pięknoŃĘ twU w całeA ozdobie widzę i opisÓAę bo tęsknię po tobie panno Ńwięta co AasneA bronisz częstocKowX i w ostreA Ńwiecisz braDie tX co TrHd zaDkowX nowoTrHdzki ocKraniasz z AeTo wiernXD CÓdeD Aak Dnie dziecko do zdrowia powrHciłaŃ cÓdeD TdX od płaczUceA Datki pod twoAU opiekę oSiarowanX DartwU podniosłeD powiekę i zaraz DoTłeD pieszo do twXcK ŃwiUtXF proTÓ iŃĘ za wrHcone ZXcie podziękowaĘ boTÓ tak nas po-wrHcisz cÓdeD na oAczXznX łono tXDczaseD przenoŃ DoAU dÓszę ÓtęsknionU do tXcK paTHrkHw CeŃnXcK do tXcK łUk zieConXcK szeroko nad błękitnXD nieDneD rozciUTnionXcK do tXcK pHc DaCowanXcK zboZeD rozDaiteD wXzła-canXcK pszenicU posrebrzanXcK ZXteD Tdzie bÓrsztXnowX Ńwierzop TrXka Aak ŃnieT biała Tdzie panieFskiD rÓDieFceD dziecięCina pała a wszXstko przepasane AakbX wstęTU DiedzU zieConU na nieA z rzadka cicKe TrÓsze siedzU

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	?	B	I	?	P	J	W	?	?	?	'_'	?	A ₂	?	Ĉ	?
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
E	?	G	?	Ł	M	N	?	O	?	R	?	?	Y	?	?	Ž

- szukamy słów pozwalających jednoznacznie określić podstawienia,

C = **Citwo** oAczXzno DoAa tX Aesteń Aak zdrowie iCe cię trzeba cenię ten tXCko się dowie kto cię stracił **dziń pięknońE** twU w **całeA** ozdobie widzę i opisóAę bo tęsknię po tobie panno Ńwięta co AasneA bronisz częstocKowX i w ostreA Ńwiecisz **braDie** tX co TrHd zaDkowX nowoTrHdzki ocKraniasz z AeTo wiernXD CÓdeD Aak Dnie dziecko do zdrowia powrHciłań cÓdeD TdX od płaczUceA Datki pod twoAU opiekę oSiarowanX DartwU podniosłeD powiekę i zaraz DoTłeD pieszo do twXcK ŃwiUtXF proTÓ ińE za wrHcone ZXcie podziękowaę boTÓ tak nas powrHcisz cÓdeD na oAczXznX łono tXDczaseD przenoń DoAU dÓszę ÓtęsknionU do tXcK paTHrkHw CeńnXcK do tXcK łUk zieConXcK szeroko nad błękitnXD nieDneD rozciUTnionXcK do tXcK pHc DaCowanXcK zboZeD rozDaiteD wXzła-canXcK pszenicU posrebrzanXcK ZXteD Tdzie bÓrsztXnowX Ńwierzop TrXka Aak ŃnieT biała Tdzie panieFskiD rÓDieFceD dzięcieCina pała a wszXstko przepasane AakbX wstęTU DiedzU zieConU na nieA z rzadka cicKe TrÓsze siedzU

- wykonujemy oczewiste podstawienia: $C \mapsto l, A \mapsto j, X \mapsto y, D \mapsto m, \acute{N} \mapsto \acute{s}, E \mapsto \acute{c},$

Tekst jawny (podstawienie X):

C = litwo ojczyzno moja ty jesteś jak zdrowie ile cię trzeba cenić ten tylko się dowie kto cię stracił dziś piękność twą w całej ozdobie widzę i opisuję bo tęsknię po tobie panno święta co jasnej bronisz częstokroć i w ostrej świecisz bramie ty co Trzód zamkowy nowo Trzódki okraniasz z jeTo wiernym lódem jak mnie dziecko do zdrowia powróciłaś cōdem Tdy od płaczUcej matki pod twoją opiekę oSiarowany martwU podniosłem powiekę i zaraz moTłem pieszo do twych świętych proTó iść za wrócone Zycie podziękować boTó tak nas powrócisz cōdem na ojczyzny łono tymczasem przenoś moją dōszę ótęsknionU do tych paTHrkHw leśnych do tych łuk zielonych szeroko nad błękitnym niemnem rozciUTnionych do tych pól malowanych zbożem rozmaitem wyłaczanych pszenicU posrebrzanych Zytem Tdzie bōrsztynowy świerzop Tryka jak śnieT biała Tdzie panieFskim rōmieFcem dzięcielina pała a wszystko przepasane jakby wstęTU między zielonU na niej z rzadka cienie Trósze siedzą

- co już wiemy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	?	B	I	Ę	P	J	W	?	?	?	'_'	A	Ą	C	Ć	D
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
E	?	G	?	Ł	M	N	Ń	O	?	R	?	X	Y	?	?	Ż

- analizujemy niepełną tabelę podstawień i ustalamy słowo kluczowe $\alpha = \text{LUBIĘPJWSTK}'_{'}$, wtedy:

a	ą	b	c	ć	d	e	ę	f	g	h	i	j	k	l	ł	m
L	U	B	I	Ę	P	J	W	S	T	K	'_'	A	Ą	C	Ć	D
n	ń	o	ó	p	r	s	ś	t	u	w	x	y	z	ż	ź	' '
E	F	G	H	Ł	M	N	Ń	O	Ó	R	Ś	X	Y	Z	Ż	Ź

Tekst tajny:

P = litwo ojczyzno moja ty jesteś jak zdrowie ile cię trzeba cenić ten tylko się dowie
kto cię stracił dziś piękność twą w całej ozdobie widzę i opisuję bo tęsknię po tobie
panno święta co jasnej bronisz częstochowy i w ostrej świecisz bramie ty co gród
zamkowy nowogródzki ochraniasz z jego wiernym ludem jak mnie dziecko do zdro-
wia powróciłaś cudem gdy od płaczącej matki pod twoją opiekę ofiarowany martwą
podniosłem powiekę i zaraz mogłem pieszo do twych świątyń progu iść za wrócone
życie podziękować bogu tak nas powrócisz cudem na ojczyzny łono tymczasem prze-
noś moją duszę utęsknioną do tych pagórków leśnych do tych łąk zielonych szeroko
nad błękitnym niemnem rozciągnionych do tych pól malowanych zbożem rozma-
item wyłaczanych pszenicą posrebrzanych żytem gdzie bursztynowy świerzop gryka
jak śnieg biała gdzie panieńskim rumieńcem dzięcielina pała a wszystko przepasane
jakby wstęgą miedzą zieloną na niej z rzadka ciche grusze siedzą