

SR HJLHZ HPRHD XZQD FHJON JGHJ YGJAN SR AHZPNIE FQRA
CPJMRFRQ DXR OZIRGSJ. B ZADJS FQRAY XZQZ IJGHZY FDORH SR
MSZENIE MDJGHRIE PZXZHSDAZF AHZPD OZAZSIZFRQD GHRFXN
HYSJQZF RQJXZ FDROYAHZF RQJXZ ZCPRFZFRQD CZGAZOJSJ YGJAN
HPRHJ. RA PZXZHSDID SJCPRIZFRQD XQDBAZ SJLRAJL ZGRON
AHZPJ GR HY FHJON MSZBDQD RAZ EYXN CZ ORBOD ZXNIRLSJ GD
GHRFRQD HRXZPN R HZ RL G ZCJFSJSJM. XZQZ HZ CZHPJXSJ QJXZ
HYSRLGD DSODRSD CZAQRORQD GHRFXN HPRHJ BR BRGRE OZ
GFZLDIE CPRF R CPJHZ GR GSRBDQD FGJHANMD GCZGZXMD CPRIY
ERHDH R BSJMZBSDH.

Hypotézy:

1. $R = \mathbf{A}$ (lebo R je najfrekventovanejšie písmeno a vyskytuje sa aj samostatne)
2. $Z = \mathbf{O}$ (lebo Z je druhé najfrekventovanejšie písmeno)

SA HJLHO HPAHD XOQD FHJON JGHJ YGJAN SA AHOPNIE FQAA CPJM
AFAQ DXA OOIAGSJ. B OADJS FQAAY XOQO IJGHOY FDOAH SA
MSOENIE MDJGHAIE POXOHSDAOF AHOPD OOAOSIOFAQD GHAFXN
HYSJQOF AQJXO FDAOYAHOF AQJXO OCPAFOFAQD COGAOOJSJ YGJAN
HPAHJ. AA POXOHSDID SJCPAIOFAQD XQDBAO SJLAAJL OGAON
AHOPJ GA HY FHJON MSOBDQD AAO EYXN CO OABOD OXNIALSJ GD
GHAFQD HAXOPN A HO AL G OCJFSJS DM. XOQO HO COHPJXSJ
QJXO HYSALGD DSODASD COAQAOAQD GHAFXY HPAHJ BA BAGAE OO
GFOLDIE CPAF A CPJHO GA GSABDQD FGJHANMD GCOGOXMD CPAIY
EAHDH A BSJMOBSDH.

Ďalšie hypotézy:

3. $S = N$ (lebo v texte sa viackrát vyskytuje SA – predložka “NA” a písmeno S je v šifrovom texte na 6. mieste a N je v slovenčine na 5. mieste)
4. $H = T$ (lebo H je na 3. mieste a T v slovenčine na 7. mieste – avšak tesne za 4. – a zároveň máme v texte viekrát HO, čo môže byť „TO“)

NA TJLTO TPATD XOQD FTJON JGTJ YGJAN NA ATOPNIE FQAA CPJM
AFAQ DXA OOIAGNJ. B OADJN FQAAY XOQO IJGTOY FDOAT NA
MNOENIE MDJGTAIE POXOTNDAOF ATOPD OOAONIOFAQD GTAFXN
TYNJQOF AQJXO FDAOYATOF AQJXO OCPAFOFAQD COGAOOJNJ YGJAN
TPATJ. AA POXOTNDID NJCPAIOFAQD XQDBAO NJLAAJL OGAON
ATOPJ GA TY FTJON MNOBDQD AAO EYXN CO OABOD OXNIALNJ GD
GTAFQD TAXOPN A TO AL G OCJFNJNDM. XOQO TO COTPJXNJ
QJXO TYNALGD DNODAND COAQAOAQD GTAFX Y TPATJ BA BAGAE OO
GFOLDIE CPAF A CPJTO GA GNABDQD FGJTANMD GCOGOXMD CPAIY
EATDT A BNJMOBNDT.

Ďalšie hypotézy:

5. D alebo J by mali byť *E*, lebo sú to posledné dosť frekventované znaky v šifrovom texte a E je významným znakom v slovenčine. Ak si všimneme v druhom riadku kombináciu *DXA* a v šiestom *GD* – usúdime, že $J = E$.
6. Takže nám ostalo písmeno D, frekvenčne “vyčnievajúce”. Pravdepodobne bude za ním “skrytý” znak *I* alebo *S*. Keďže asi ťažko nájdeme dvojpísmenové slovo tak aby končilo na *I* (viz. “GD” v 6. riadku) a koncovka posledného slova je skôr *NIT* ako *NST*, bude naša voľba $D = I$.

NA TELTO TPATI XOQI FTEON EGTE YGEAN NA ATOPNIE FQAA CPEM
AFAQ IXA OOIAGNE. B OAIEN FQAAY XOQO IEGTOY FIOAT NA
MNOENIE MIEGTAIE POXOTNIAOF ATOPI OOAONIOFAQI GTAFXN
TYNEQOF AQEXO FIAOYATOF AQEXO OCPAFOFAQI COGAAOENE YGEAN
TPATE. AA POXOTNIII NECPAIOFAQI XQIBAO NELAAEL OGAON
ATOPE GA TY FTEON MNOBIQI AAO EYXN CO OABOI OXNIALNE GI
GTAFQI TAXOPN A TO AL G OCFNENIM. XOQO TO COTPEXNE
QEXO TYNALGI INOIANI COAQAOQI GTAFXI TPATE BA BAGAE OO
GFOLIE CPAF A CPETO GA GNABIQI FGETANMI GCOGOXMI CPAIY
EATIT A BNEMOBNIT.

Teraz sme v stave, keď môžeme priamo „hádat“ písmená zo slov:

1. riadok nám dá: $L = J$ $P = R$ $G = S$
8. riadok nám dá: $O = D$

**NA TEJTO TRATI XOQI FTEDN ESTE YSEAN NA ATORNIE FQAA CREM
AFAQ IXA DOIASNE. B OAIEN FQAAY XOQO IESTOY FIDAT NA
MNOENIE MIESTAIE ROXOTNIAOF ATORI DOAONIOFAQI STAFXN
TYNEQOF AQEXO FIADYATOF AQEXO OCRAFOFAQI COSAODENE YSEAN
TRATE. AA ROXOTNIII NECRAIOFAQI XQIBAO NEJAAEJ OSADN
ATORE SA TY FTEDN MNOBIQI AAO EYXN CO DABDI OXNIAJNE SI
STAFQI TAXORN A TO AJ S OCFNENIM. XOQO TO COTREXNE
QEXO TYNAJSI INDIANI COAQADAQI STAFXI TRATE BA BASAE DO
SFOJIE CRAF A CRETO SA SNABIQI FSETANMI SCOSOXMI CRAIY
EATIT A BNEMOBNIT.**

Pokračujeme v „hádání“ písmen zo slov:

2. riadok nám dá:	X = B	I = C	F = V
4. riadok nám dá:	A = K	N = Y	
6. riadok nám dá:	C = P	B = Z	
9. riadok nám dá:	Q = L		

**NA TEJTO TRATI BOLI VTEDY ESTE YSEKY NA KTORYCE VLAK PREM
AVAL IBA DOCASNE. Z OKIEN VLAKY BOLO CESTOY VIDAT NA
MNOEYCE MIESTACE ROBOTNIKOV KTORI DOKONCOVALI STAVBY
TYNELOV ALEBO VIADYKTOV ALEBO OPRAVOVALI POSKODENE YSEKY
TRATE. AK ROBOTNICI NEPRACOVALI BLIZKO NEJAKEJ OSADY
KTORE SA TY VTEDY MNOZILI AKO EYBY PO DAZDI OBYCAJNE SI
STAVALI TABORY A TO AJ S OPEVNENIM. BOLO TO POTREBNE
LEBO TYNAJSI INDIANI POKLADALI STAVBY TRATE ZA ZASAE DO
SVOJICE PRAV A PRETO SA SNAZILI VSETKYMI SPOSOBMI PRACY
EATIT A ZNEMOZNIT.**

Teraz je to už naozaj veľmi jednoduché.

Zvyšné substitúcie: $Y = U$, $E = H$, $M = M$

NA TEJTO TRATI BOLI VTEDY ESTE USEKY NA KTORYCH VLAK
PREMAVAL IBA DOCASNE. Z OKIEN VLAKU BOLO CESTOU VIDAT NA
MNOHYCH MIESTACH ROBOTNIKOV KTORI DOKONCOVALI STAVBY
TUNELOV ALEBO VIADUKTOV ALEBO OPRAVOVALI POSKODENE USEKY
TRATE. AK ROBOTNICI NEPRACOVALI BLIZKO NEJAKEJ OSADY
KTORE SA TU VTEDY MNOZILI AKO HUBY PO DAZDI OBYCAJNE SI
STAVALI TABORY A TO AJ S OPEVNENIM. BOLO TO POTREBNE
LEBO TUNAJSI INDIANI POKLADALI STAVBU TRATE ZA ZASAH DO
SVOJICH PRAV A PRETO SA SNAZILI VSETKYMI SPOSOBMI PRACU
HATIT A ZNEMOZNIT.

Šifrový kľúč (permutácia):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
R X I O J ? ? E D L A Q M S Z C ? P G H Y F ? ? N B